JOURNAL OF ALGEBRA 79, 9–36 (1982)

Complex Linear Groups of Degree at Most $(q-1)/2$

PAMELA A. FERGUSON

Department of Mathematics, University of Miami, Coral Gables, Florida 33124

Communicated by Walter Feit

Received October 20, 1981

INTRODUCTION

A finite group G with Sylow p subgroup P satisfies *Hypothesis 1* if $C_G(x) = C_G(P)$ for all $x \in P^{\#}$.

The following theorem has been conjectured.

CONJECTURED THEOREM. *Assume G satisfies Hypothesis 1 and G has a faithful complex character Λ of degree at most $\frac{1}{2}(|P|-1)$. Then either $P \trianglelefteq G$ or $G/Z(G) \simeq PSL(2, |P|)$.*

Brauer [1] proved this theorem in the case that $|P| = p$. It follows from Sibley's theorem 2 [10] that $P \trianglelefteq G$ if $\Lambda(1) < (|P|-1)/2$. The theorem has also been proved [3] if $N_G(P)/C_G(P)$ is cyclic. In this paper, we prove the following specialized version of the conjectured theorem.

THEOREM 1. *Assume G is a finite group with a Sylow p group P satisfying $C_G(x) = P$ for all $x \in P^{\#}$. If G has a faithful complex character Λ of degree at most $\frac{1}{2}(|P|-1)$, then either $P \trianglelefteq G$ or $G/Z(G) \simeq PSL(2, |P|)$.*

In general, it is difficult to determine the multiplicities of irreducible characters in a product of characters. However, if G is a minimal counterexample to Theorem 1, then it is possible. The determination of these multiplicities is crucial for showing that G does not exist. In order to obtain these multiplicites, it is necessary to determine the irreducible characters of $N_G(P)/C_G(P)$. Hence, it is necessary to know the structure of $N_G(P)/C_G(P)$ in some detail. This structure is discussed in Section 2.

The results in Sections 1 and 2 are stated in a more general form than are needed to prove Theorem 1. This is done because hopefully these results will be useful in proving the general case of the conjectured theorem. In Section 1, it is shown that if G is a minimal counterexample to the conjectured theorem, then $G/Z(G)$ is simple. However, the purpose of this paper is to

0021-8693/82/110009–28$02.00/0

prove Theorem 1 by using results about Frobenius groups and character theoretic arguments rather than to appeal to the classification of finite simple groups.

1

A group G satisfies *Hypothesis* 1$'$ if the following conditions are satisfied: (i) G satisfies the hypothesis but not the conclusion of the conjectured theorem: (ii) if K is a proper normal subgroup of G containing $C_G(P)$, then either $P \triangle K$ or $K/Z(K) \simeq PSL(2, |P|)$. Throughout, this section we assume that G satisfies Hypothesis 1$'$.

Let N and V denote respectively the normalizer of P in G and the group of p' elements in $C_G(P)$. N/V is a Frobenius group and $C_G(P) - V$ is a TI set in G. Let E denote a complement of P in N. Let $q = |P|$ and $n = |N|/|C_G(P)| = |E|/|V|$.

As noted in the Introduction, $\Lambda(1) = (q-1)/2$ and E/V is non-abelian if G satisfies Hypothesis 1$'$. In particular, P is not cyclic.

If Λ were reducible, then Sibley's theorem [10] could be applied to the constituents of Λ to show that $P \trianglelefteq G$. Therefore, Λ is irreducible.

We use the notation of Leonard [7]. In addition, let $(q-1)/n = t$.- $\Lambda(1) = (q-1)/2$ and Λ faithful imply that $t \geqslant 2$. If Λ is not exceptional, then it follows from Section 1 [7] that $\Lambda(g) \equiv \Lambda(1) \pmod q$ for $g \in P^{\#}$ and $\Lambda^2(g) < n$. Hence, $\Lambda(1) = (q-1)/2$ implies that Λ is an exceptional character. As in Section 1(E) [7], we may assume that $\Lambda = \Lambda_k$ lies in some block $\mathscr{B}_i$. It also follows from Section 1 [7] that there are non-negative integers a_i, b_i and u such that $\Lambda(1) = (a_i + \varepsilon_i)\,\psi_i(1)n + a_i\psi_i(1)n(((q-1)/n_i) - 1) + b_i(n/n_i)\,\psi_i(1) + uq$. Moreover, $\varepsilon_i = \pm 1$, $a_i + \varepsilon_i \geqslant 0$, and we may assume $\varepsilon_i = 1$ if $t = 2$. $\Lambda(1) = (q-1)/2$ implies that $u = 0$.

Assume that $t \geqslant 3$, then $n(((q-1)/n_i) - 1) > (q-1)/2$ so that $a_i = 0$. In this case, Theorem 1 [10] implies that $\Lambda = (\psi_i \lambda_{ik})^N$. However, a careful reading of Sibley's paper [10] shows that he proved that $P \triangle G$ under these conditions. Therefore, $t = 2$ if G satisfies Hypothesis 1$'$. Now $\varepsilon_i = 1$ and $\Lambda(1) = (q-1)/2 = n$ imply that $a_i = b_i = u = 0$, and $\psi_i(1) = 1$. In particular, Λ_N is irreducible. Since Λ is faithful, V is abelian.

We next show that if K is a proper normal subgroup of G which contains V, then $K = V$. P is not cyclic. Thus, if $(|K|, p) = 1$, then Theorem 5.3.16 [5] may be applied to the Sylow subgroups of K to show that $K = V$. If $(|K|, p) \neq 1$, then $n = (q-1)/2$ implies that $P \subseteq K$. Therefore, K is a finite group with Sylow p subgroup P such that $C_G(x) = C_G(P)$ for all $x \in P^{\#}$. Moreover, Λ_K is a faithful complex character of K of degree $(|P| - 1)/2$. Since $|K| < |G|$, Hypothesis 1$'$(ii) implies that $P \trianglelefteq K$ or $K/Z(K) \simeq PSL(2, |P|)$. However, the Frattini argument implies that $G = NK$. Hence, $P \ntrianglelefteq K$. If $K/Z(K) \simeq PSL(2, |P|)$, then $|N_K(P)/C_K(P)| = (|P| - 1)/2 =$

$|N/C_G(P)|$. However, $C_K(P) = C_G(P)$ since $PV \subseteq K$. It follows that $N \subseteq K$. Now $G = NK$ contradicts $|K| < |G|$.

Λ_N is irreducible and V is abelian. Therefore, the method of proof used in Lemma 2 [3] may be combined with the previous paragraph to show that $V = Z(G)$ and $G/Z(G)$ is simple. Thus, [4] now implies that $p \neq 3$.

We summarize our results in the following proposition.

PROPOSITION 1. *Assume that G satisfies Hypothesis 1′. Then $C_G(P) = Z(G) \times P$, $|N/C_G(P)| = (q-1)/2$, $p \neq 3$, Λ is an exceptional character, Λ_N is irreducible character which is induced from a character of $C_G(P)$, and $G/Z(G)$ is a simple group.*

2

A group EP satisfies *Hypothesis 2* if EP is a Frobenius group with kernel P, E is a non-abelian complement, $(|P|, 3) = 1$, and $|E| = (|P|-1)/2$.

Assume EP satisfies Hypothesis 2. E non-abelian and $|E| = (|P|-1)/2$ imply that P is a non-cyclic elementary abelian p group.

LEMMA 2.1. *Assume EP satisfies Hypothesis 2. If C is a cyclic normal subgroup of E, then there are positive integers a, b such that $|C|$ divides $p^a - 1$ and $|P| = p^{ab}$. If $C_E(C)$ is not abelian, then $b \geqslant 2$.*

Proof. Since P is an elementary abelian p-group, we may view P as a vector space V of order $|P|$ over a field F where $|F| = p$. Now $|E| = (|P|-1)/2$ implies that V is a faithful irreducible $F[E]$ module. Let W denote an irreducible $F[C]$ module. Theorem 6.5 [6] implies that $V = \oplus\sum_{i=1}^{b} W_i$ where the W_i are irreducible $F[C]$ modules conjugate to W. Since C acts faithfully on W, $|W| = p^a = 1 + c|C|$. Moreover, $|P| = p^{ab}$. If $b = 1$, then C acts irreducibly on V. Proposition 19.8 [9] implies that $C_E(C)$ is abelian. ($T(q^n)$ is defined on p. 229 of [9]. It is direct to show that the subgroup of $T(q^n)$ consisting of linear transformations is abelian.) Therefore, $b \geqslant 2$ if $C_E(C)$ is non-abelian.

If K is a group, let $F(K)$ denote the Fitting subgroup of K.

A Z-group is a group in which every Sylow subgroup is cyclic. Assume that E_0 is a subgroup of E and E_0 is a Z-group. The proof of Theorem 18.2 [9] implies that $E_0 = RE_0'$, where E_0' denotes the commutator subgroup of E_0. Moreover, R and E_0' are cyclic Hall subgroups of E_0, $R \cap E_0' = 1$ and $Z(E_0) \subseteq R$. $F(E_0) = Z(E_0) \times E_0'$, $Z(E_0) = R \cap F(E_0)$, $E_0/F(E_0)$ is isomorphic to a cyclic subgroup of $\mathrm{Aut}(E_0')$, and every prime dividing $|E_0/E_0'|$ divides $|Z(E_0)|$. This information will be used repeatedly in the following lemmas.

LEMMA 2.2. *If EP satisfies Hypothesis 2, then E is solvable.*

Proof. We will will assume E is not solvable. Theorem 18.6 [9] implies that E contains a normal subgroup E_0 with $|E/E_0| \leqslant 2$ such that $E_0 = K_0 \times M$, M is a Z-group of order relatively prime to 30, and $K_0 \simeq SL(2, 5)$. We may choose notation so that $E = KM$ where $(|K|, |M|) = 1$, $M \triangle E$, and $K_0 \subseteq K$.

P non-cyclic and $|P| = 2|E| + 1$ imply that $|M| \neq 1$. Let $F(M) = C$ and $|M/F(M)| = j$. Since M is a non-trivial Z-group of order relatively prime to 30, $|Z(M)| \geqslant 7$. It follows that $|C| \geqslant 14j$ if $j \neq 1$. C is a normal cyclic subgroup of E of odd order and $C_E(C) \supseteq K_0$. Therefore, Lemma 2.1 implies that there are integers a, b such that $p^a = 1 + 2c|C|$, $|P| = p^{ab}$, and $b \geqslant 2$. We note that $1 + 2c|C| \neq 15$. Since $|P| = 1 + 2|E|$, it follows that $(2c|C|)^b < |P| - 1 = 2|K|j|C| \leqslant 2^5 15j|C|$. $|C| \geqslant 14j$ if $j \neq 1$ and $1 + 2c|C| \neq 15$ imply that $b = 2$. Since every prime dividing j divides $|C|$ and $(p^a - 1, p^a + 1) = 2$, we see that $p^a - 1 = 2c'|M|$. Moreover, $2|K| = 4c'(c'|M| + 1)$ where $|K| = 120$ or 240. Computations using the conditions on M now imply that $(|M|, |P|) = (13, 79^2)$ or $(119, (239)^2)$ and $|K| = 240$.

Thus, E and in particular K is isomorphic to a subgroup of $GL(2, p)$ where $p = 79$ or 239. Since p is not a factor of $|K| = 240$, this implies that K has a faithful complex representation of degree 2. But $2 = (5-1)/2$ and $240 = 2^4 \cdot 3 \cdot 5$, so Brauer's special theorem [1] applied to the prime 5 implies that $K_5 \triangle K$. This is a contradiction.

Let Z_1 denote the Hall $2'$ subgroup of $Z(E)$.

LEMMA 2.3. *If EP satisfies Hypothesis 2 and $F(E)_2$ is generalized quaternion, then one of the following conditions is satisfied*:

(i) $|P| = 49$ and $E/Z(E) \simeq A_4$.

(ii) $|P| = 47^2$ and $E = K \times Z_1$, where $|Z_1| = 23$, and $K/Z(K) \simeq S_4$.

(iii) $|P| = 23^2$ and $E = K \times Z_1$, where $|Z_1| = 11$, and $K/Z(K) \simeq A_4$.

(iv) E has a normal cyclic subgroup of index 2.

Proof. If $|P| = 49$, then clearly (i) or (iv) is satisfied. We will assume $|P| \neq 49$. Let d be defined by $|F(E)_2| = 2^d$. The proof of Theorem 18.2 [9] provides the following information. E contains a normal subgroup E_0 such that E_0 is a Z-group and $E_0 = C_E(W)$ where W is a characteristic subgroup of $F(E)_2$. Let the index of E_0 in E be denoted by r. If $d \geqslant 4$, then $|W| \geqslant 8$, W is cyclic, and $r = 2$. If $d = 3$, then $|(E_0)_2| = 2$, $4 | r$, $r | 24$, and E/E_0 is isomorphic to a subgroup of S_4.

Let C denote the Hall $2'$ subgroup of $F(E_0)$. If $|C| = 1$ and $d = 3$, then $|P| = 1 + 4r$. Since P is not cyclic, conditions on r imply that $|P| = 49$. If $|C| = 1$ and $d \geqslant 4$, then $E = E_2, |E| \geqslant 2^4$, and $|P| = 1 + 2^j$. Since P is not cyclic, $|C| \neq 1$ if $d \geqslant 4$. Thus, we may assume $|C| \neq 1$. Let j denote the order of a Hall $2'$ subgroup of $E_0/F(E_0)$, then $|E_0|=j|E_0|_2|C|$. Since E_0 is a Z-group and $|C|\neq 1$, $|C|^2 \geqslant 3j$. Moreover, every prime dividing j divides $|C|$.

C is a cyclic normal subgroup of E, hence $C\subseteq F(E)$. Since $F(E)$ is non-abelian and $|C|$ is odd, Lemma 2.1 implies that there are integers a, b such that $2|C|\,|\,p^a-1$, $|P|=p^{ab}$, and $b\geqslant 2$. If b is divisible by an odd prime v, then $|P|^{1/v}=p^{ab/v}$ is an integer and $\sum_{j=0}^{v-1}(|P|^{1/v})^j$ is odd. It now follows from $|P|=1+2|E|$ that $2|E_2|\ |C|$ divides $|P|^{1/v}-1$. In particular, $2|E_2|\,|C|\leqslant |P|^{1/3}-1$. However, $r\leqslant (|E_2|, r)\,3$ and $2|E|=2r|E_0|_2 j|C|$ now imply that $(2|E_2|\,|C|)^3<|P|-1\leqslant 2\cdot 3|E_2|\,j|C|$. This contradicts $|C|^2\geqslant 3j$. Thus, b is a power of 2 and $|P|=p^{2a'}$ where $|C|\,|\,p^{a'}-1$. Since every prime dividing j divides $|C|$ and $(p^{a'}-1, p^{a'}+1)=2$, $2j|C|$ divides $p^{a'}-1$. $|P|=1+2r|E_0|_2 j|C|$ and $r=(r,|E_2|)(r,3)$ now imply that $p^{a'}+1$ divides $(r,3)\,|E_2|$.

If $p^{a'}+1\,\big|\,|E_2|$, then $p^{a'}\equiv 3 \pmod 4$ so it follows that $p^{a'}+1=|E_2|=2^s$. But $1+p^{a'}=2^s$ implies that $a'=1$, whence $|P|=p^2$. If $d\geqslant 4$, then $|W|\geqslant 8$ so that $|W|\nmid p-1$. However, W is a normal cyclic subgroup of E. Since $|P|=p^2$ and $|W|\nmid p-1$, Lemma 2.1 implies that $C_E(W)=E_0$ is abelian if $d\geqslant 4$. In particular, E_0 is cyclic and $r=2$ if $d\geqslant 4$ so that (iv) is satisfied. If $d=3$ and $p^{a'}+1=|E_2|$, then $|E_2|=8$ or 16 implies that $|P|=49$.

Thus, we may assume $p^{a'}+1\mid (3,r)\,|E_2|$ where $(r,3)=3$. Therefore $d=3$ and we assume that $|P|\neq 49$. It now follows from $p^{a'}+1\,\big|\,3|E_2|$ that $p^{a'}=1+2c_1|C|\,j$ where $(c_1,2)=1$. In particular, $p^{a'}+1=3\,|E_2|$. Since $|E_2|=16$ or 8, it follows that $(|P|, |C|\,j)=(47^2, 23)$ or $(23^2, 11)$. Therefore, E is isomorphic to a subgroup of $GL(2,p)$ where $p=47$ or 23. Conditions (ii) or (iii) now easily follow from the structure of E and $GL(2,p)$ for $p=47$ or 23.

LEMMA 2.4. *Assume EP satisfies Hypothesis 2 and $F(E)_2$ is cyclic. Let $u=|E/F(E)|$, then the following conditions are satisfied.*

(i) *$E=HD$ where $(|H|,|D|)=1$, D is the Hall $2'$ subgroup of E' where E' denotes the commutator subgroup of E'. D is cyclic and H is nilpotent. $F(E)=(H\cap F(E))\times D$ and $H\cap F(E)\supseteq Z(E)$. Every prime dividing u divides $|Z(E)|$.*

(ii) $|P|=p^{ud}$.

(iii) *If R is a subgroup of E which properly contains $F(E)$, then there are integers a, b, where $b\geqslant 2$, $|C_{F(E)}(R)|\,|\,p^a-1$ and $|P|=p^{ab}$. If v is a prime dividing b, then $|C_{F(E)}(R)|\,u/(u,v)$ divides $|P|^{1/v}-1$.*

(iv) *$E/F(E)$ is cyclic. If E_2 is generalized quaternion, then $u=2u_1$ where u_1 is an odd positive integer.*

Proof. (i) If E_2 is cyclic, then (i) follows since E is a Z group. Therefore, we may assume that E_2 is generalized quaternion. The proof of

Theorem 8.2 [9] implies that $E/F(E)$ is abelian, $F(E)$ is cyclic, and E has a normal subgroup E_0 such that E/E_0 is of type 2 or (2, 2). Further, E_0 is a Z group, $E_0 \supseteq F(E)$, and $(E_0)_2 = F(E)_2$. Since E_0 is a Z-group, $E_0 = AE_0'$, A and E_0' are cyclic, $(|A|, |E_0'|) = 1$, and $Z(E_0) \subseteq A$. It follows that E_0' is a Hall subgroup of E of odd order.

Let R be a Hall m subgroup of E where $m = |E/E_0'|$. Let R_1 be a Hall $2'$ subgroup of R. If $\tilde{R} = R \cap E_0$, then notation may be chosen so that $\tilde{R} = A$. Then, R_1 is the cyclic normal $2'$ subgroup of $\tilde{R}$. Hence R_1 is a cyclic normal subgroup of R. Since every Sylow subgroup of R_1 is cyclic, Theorem 5.2.3 [5] implies that $R_1 = C_{R_2}(R_1) \times [R_2, R_1]$ where R_2 is a Sylow 2 subgroup of R. Let $H = R_2 C_{R_2}(R_1)$ and $D = [R_2, R_1] E_0'$. By construction H is nilpotent, $(|H|, |D|) = 1$, and $E = HD$. Moreover, H nilpotent implies that $E' = H_2' \times D$ where H_2' denotes the commutator subgroup of H_2. The remaining statements in (i) follow directly from the construction of H and D and properties of Frobenius complements.

(ii) Since E is solvable and non-abelian, $E/F(E)$ is isomorphic to a subgroup of $\mathrm{Aut}(F(E)/Z(E))$. Therefore, $u \leqslant (|F(E)/Z(E)| - 1) \leqslant |F(E)|/2 - 1$. Lemma 2.1 implies that there are positive integers a, b such that $|P| = p^{ab}$ and $|F(E)| \mid p^a - 1$ since $F(E)$ is cyclic. Now $|E| = u|F(E)|$ implies that $|F(E)|^b \leqslant |P| - 1 = 2u|F(E)| \leqslant 2(|F(E)|/2 - 1)|F(E)|$, whence $b = 1$.

We may view P as a vector space of order p^a. Proposition 19.8 [9] implies that E is isomorphic to a subgroup of $T(p^a)$. Moreover, $C_E(F(E))$ is isomorphic to a subgroup of T_1 where T_1 is the subgroup of $T(p^a)$ consisting of linear transformations. Using the definition of $T(p^a)$ on p. 229 of [9], we see that T_1 is abelian and $|T(p^a)/T_1| = a$. Since E is solvable $C_E(F(E)) = F(E)$. Therefore, T_1 abelian implies that $|E/F(E)| = u$ divides a. Therefore, $|P| = p^a = p^{ud}$.

(iii) For ease of notation, let $C = C_{F(E)}(R)$, then C is a normal cyclic subgroup of E. ($F(E)$ is cyclic.) Since R properly contains $F(E)$ and E is solvable, R is non-abelian. Therefore, Lemma 2.1 implies there are integers a, b, such that $|C| \| p^a - 1$, $b \geqslant 2$, and $|P| = p^{ab}$.

Let v be a prime divisor of b. If v divides u, let h be defined by $u = hv^j$ where $(h, v) = 1$ and $j \geqslant 1$. It follows from (i) and (ii) of this lemma that $|P| = p^{hdv^j}$ and $|E_v| \geqslant v^{j+1}$. Now $p^{hdv^j} \equiv 1 \pmod{v^{j+1}}$ and elementary number theory imply that $p^{hd} \equiv 1 \pmod{v}$. It follows that $|P|^{1/v} = p^{hdv^{j-1}} \equiv 1 \pmod{v^j}$. In particular, $(u, |E_v|)$ divides $|P|^{1/v} - 1$.

$|P| = p^{ab}$ and $|C| \mid p^a - 1$ imply that $|C| \mid |P|^{1/v} - 1$ if v is a prime divisor of b. $(\sum_{j=0}^{v-1} (|P|^{1/v})^j, |P|^{1/v} - 1)$ divides v. Hence, if $(|E_v|, u) \geqslant v^2$, the previous paragraph and $|P| = 1 + 2|E| = 1 + 2u|F(E)|$ imply that $((u, |E_v|)|C_v|/v) \mid |P|^{1/v} - 1$. If $(|E_v|, u) \leqslant v$, this result follows trivially. If v' is a prime unequal to v which divides u, then part (i) implies that

$|Z(E)_{v'}| \neq 1$. In particular, $|C_{v'}| \neq 1$ so $(|P|^{1/v} - 1, \sum_{j=0}^{v-1} (|P|^{1/v})^j)|v$ implies that $|C_{v'}|(u, |E_{v'}|)\,\big|\,|P|^{1/v} - 1$. Part (iii) follows.

(iv) Part (iv) follows immediately from (i) unless E_2 is generalized quaternion. As noted in the proof of (i), if E_2 is quaternion, then $E_2/F(E)_2$ is of type 2 or (2, 2). It is sufficient to show that the latter case may not occur. We will assume that $E_2/F(E)_2$ is of type (2, 2), whence $u = 4u_1$ where u_1 is an odd integer.

Let $L = F(E)\,E_2$, and let R_i, $i = 1, 2, 3$, denote the distinct subgroups of index 2 in L which contain $F(E)$. Let $C_i = C_{F(E)}(R_i)$ for $i = 1, 2, 3$. E_2 generalized quaternion, $F(E)$ cyclic and $L/F(E)$ of type (2, 2) imply that $F(E)_2 \subseteq C_i$ for some i and $|C_{F(E)_2}(R_j)| = 2$ if $j \neq i$. Let F_r denote a Sylow r subgroup of $F(E)$ where $r \neq 2$. Since F_r is cyclic and $L/F(E)$ is of type (2, 2), Theorems 5.3.16 and 5.3.2 of [5] imply that $F_r \subseteq C_i$ for some i. Moreover, if $r|(|C_i|, |C_j|)$ where $i \neq j$, then $|F_r|\,\big|\,|C_{C(E)}(L)|$. Let k denote the order of the Hall $2'$ subgroup of $C_{F(E)}(L)$, then $|C_{F(E)}(L)| = 2k$. It follows that $|F(E)| = \prod_{i=1}^{3} |C_i|/(2k)^2$. Moreover, $|P| - 1 = 2\,|E| = 8u_1|F(E)|$ so we obtain

$$|P| - 1 = \frac{2u_1 \prod_{i=1}^{3} |C_i|}{k^2}. \tag{2.4.1}$$

We choose notation so that $|C_1| \geqslant |C_2| \geqslant |C_3|$. Since R_i properly contains $F(E)$, part (iii) implies that there are integers a_i, b_i for $i = 1, 2, 3$ such that $|C_i|\,|\,p^{a_i} - 1$, $|P| = p^{a_i b_i}$, and $b_i \geqslant 2$.

If v is an odd prime divisor of b_1, then $|P|^{1/v}$ is an integer and $|P| - 1/|P|^{1/v} - 1$ is odd. It follows from $2\,|E| = |P| - 1$ and part (iii) that $(2u_1|E_2||C_1|/(u_1, v)(|E_2|, |C_1|))\big|\,|P|^{1/v} - 1$. Therefore (2.4.1) implies that $(2u_1|E_2|\,|C_1|/(u_1, v)(|E_2|, |C_1|) + 1)^v \leqslant 1 + 2u_1 \prod_{i=1}^{3} |C_i|/k^2$. However, every prime divisor of u_1 divides $|Z(E)|$, and hence divides k. Therefore, $\prod_{i=1}^{3} |C_i|/k^2 \leqslant |C_1|^3/(u_1, v)^2$. Now $v \geqslant 3$ implies a contradiction. Therefore, b_1 is a power of 2.

We are assuming that $u = 4u_1$. Hence, it follows from part (iii) that $(|C_1|u_1 4/2)\big|\,|P|^{1/2} - 1$.

Now $(|C_1|, 2) = 2$ implies that $|P|^{1/2} \equiv 1 \pmod 4$, whence $(|P|^{1/2} + 1)/2$ is odd. Equality (2.4.1) now implies that $(|P|^{1/2} + 1)/2$ divides $|C_2|\,|C_3|/k^2$. If b_i is a power of 2 for $i = 2$ or 3, then $|C_i|$ divides $|P|^{1/2} - 1$ so that $((|P|^{1/2} + 1)/2, |C_i|/k) = 1$. If v_i is an odd prime divisor of b_i, then $|P|^{1/v_i}$ is an integer and $|C_i|\,\big|\,|P|^{1/v_i} - 1$. However, $((|P|^{1/2} + 1)/2, |P|^{1/v_i} - 1)$ divides $(|P|^{1/2 - 1/v_i} + 1)/2$ and $(|P|^{1/2 - 1/v_i} + 1)/2 \leqslant ((|P|^{1/6} + 1)/2)$. It follows that $(|P|^{1/2} + 1)/2 = ((|P|^{1/2} + 1)/2,\ |C_2|\,|C_3|/k^2) \leqslant ((|P|^{1/6} + 1)/2)^2$. This is a contradiction.

In order to show that there are no groups G satisfying Hypothesis 1′, it is necessary to obtain some information about the irreducible characters of

EP/P where EP satisfies Lemma 2.4. The remaining lemma in this section will be of great use.

Assume EP satisfies Hypothesis 2. Let $\mathscr{C}$ denote the set of irreducible characters of EP/P. If $\chi_m \in \mathscr{C}$, let x_m denote the degree of χ_m and s_m denote the number of algebraic conjugates of χ_m.

LEMMA 2.5. *Assume EP satisfies Hypothesis* 2, *and* $F(E)_2$ *is cyclic. Let* $|E/F(E)| = u$.

(i) *If* $\chi_m \in \mathscr{C}$, *then* $\chi_m = \zeta^{EP}$, ζ *is a linear character of* R, *and* R *is a subgroup of* PE *containing* $F(E)\,P$. *In particular*, $x_m | u$.

(ii) *If* $\chi_m \in \mathscr{C}$ *and* $\det \chi_{m|_E} = 1_E$, *then* $Z_1 \subseteq \ker \chi_m$ *where* Z_1 *denotes the Hall* $2'$ *subgroup of* $Z(E)$.

(iii) *Let* t_u *denote the number of distinct primes dividing* u, *and let* $\mathscr{C}' = \{\chi_m | \chi_m \in \mathscr{C}$, *and* $1 \leqslant x_m < u\}$. *Then*

$$\sum_{\mathscr{C}'} x_m^2 \leqslant \frac{3t_u|E|}{|P|^{2/3}} \qquad \text{if } |P| = p^{ud} \quad \text{and} \quad (ud, 2) = 1$$

$$\leqslant \frac{4t_u|E|}{|P|^{1/2}} \qquad \text{if } |P| = p^{ud} \quad \text{and} \quad (ud, 2) = 2.$$

(iv) *If* $|E|$ *is odd, let* $\hat{\mathscr{C}} = \{\chi_m | \chi_m \in \mathscr{C}, \det \chi_m|_E = 1_E, x_m = u,$ *and* $s_m = 2\}$. Either $\hat{\mathscr{C}}$ *is empty or* $\hat{\mathscr{C}}$ *contains exactly two characters and* $1 + 2u$ *is a prime dividing* $|E|$.

Proof. The set $\mathscr{C}$ may be viewed as the set of irreducible characters of E. For ease of exposition, we shall adopt this view in this proof.

(i) Lemma 2.4 implies that $E/F(E)$ and $F(E)$ are cyclic. Let $\mathscr{I}(\Theta)$ denote the inertial group of Θ where Θ is a character of $F(E)$. Theorems 9.11 and 9.12 [2] imply there are linear characters Θ and ζ of $F(E)$ and $\mathscr{I}(\Theta)$, respectively, such that $\chi_m = \zeta^E$ and $\zeta_{F(E)} = \Theta$. (Clearly, $\chi_m = \zeta^{EP}$ if we let $R = \mathscr{I}(\Theta)\,P$.)

(ii) We assume that $\det \chi_m = 1_E$. Part (i) implies that $\chi_m = \zeta^E$ where ζ is a linear character of R and $R \supseteq F(E)$. Let H be the subgroup defined in Lemma 2.4(i), then $R = (H \cap R)\,D$. Let Z_1 denote the Hall $2'$ subgroup of $Z(E)$. A complete set of right coset representatives of R in E may be taken from H and H is nilpotent. Hence, if v is a prime dividing $|Z_1|$, then H_v is cyclic and $\chi_{m|R_v} = x_m \zeta_{R_v}$. Let $H_v = \langle w \rangle$, $R_v = \langle w_1 \rangle$ and $\ker \zeta_{R_v} = \langle w_2 \rangle$. Since H is nilpotent, $\chi_{m|H_v}$ is a character of $H_v/\langle w_2 \rangle$. Let a and b be defined by $v^a = |w/\langle w_1 \rangle|$ and $v^b = |\langle w_1 \rangle / \langle w_2 \rangle|$. Det χ_m is multiplicative and $Z(E)_v \subseteq \langle w_1 \rangle$. Therefore, it is sufficient to show that $b = 0$.

Lemma 2.4 and part (i) of this lemma imply that $x_m = |E/R| = v^a c$ where

$(v, c) = 1$. Let $\bar{K}$ denote the image of a subset K of H_v in $H_v/\langle w_2\rangle$. We choose notation so that $\mu(\bar{w}) = \alpha$ where α is a primitive v^{a+b}th root of unity, $\mu(\bar{w}_1) = \zeta(w_1)$ and μ^i, for $i = 1,\ldots, v^{a+b}$, is a full set of irreducible characters of $\langle \bar{w}\rangle$. If $a = 0$, then $1 = \det \chi_m(w_1) = (\zeta(w_1))^c$ and $(c, v) = 1$ imply that $\zeta(w_1) = 1$ so that $b = 0$. If $a \geqslant 1$, then $\chi_{m|H_v - R_v} = 0$ and $\chi_{m|R_v} = x_m \zeta_{R_v}$ imply that $X_{m|H_v} = c \sum_{j=0}^{v^a - 1} \mu^{1+jv^b}$. Therefore, $1 = \det \chi_m(w) = \alpha^{c(v^a + v^{a+b}(v^a - 1)/2)}$ Now $(c, v) = 1$ and v odd imply that $\alpha^{v^a} = 1$ so that $b = 0$.

(iii) Let $\{v_1,\ldots, v_{t_u}\}$ denote the set of distinct primes dividing u. Lemma 2.4(iv) implies that for $i = 1,\ldots, t_u$ there is exactly one subgroup R_i of E such that $R_i \supseteq F(E)$ and $[R_i : F(E)] = v_i$. If $\chi_m \in \mathscr{C}'$, then part (i) of this lemma implies that $\chi_m = \zeta^E$ where ζ is a linear character of R, and R is a subgroup of E properly containing $F(E)$. Hence, $R \supseteq R_i$ for some i. Since ζ is linear, $\langle [R_i, F(E)]\rangle \subseteq \langle [R, F(E)]\rangle \subseteq \ker \zeta$. The uniqueness of R_i now implies that $\langle [E_i, F(E)]\rangle \subseteq \ker \chi_m$.

Let $\mathscr{D}_i$ denote the set of irreducible characters of $E/\langle [R_i, F(E)]\rangle$. The previous paragraph implies that $\mathscr{C}' \subseteq \bigcup_{i=1}^{t_u} \mathscr{D}_i$. We obtain

$$\sum_{\mathscr{C}'} x_m^2 \leqslant t_u \max \left\{ \frac{|E|}{|\langle [F(E), R_i]\rangle|} \;\middle|\; i = 1,\ldots, t_u \right\}. \tag{2.5.1}$$

Let $C_i = C_{F(E)}(R_i)$ for $i = 1,\ldots, t_u$. Since $F(E)$ is cyclic, $F(E) = C_i \times [F(E), R_i]$ if v_i is odd or $v_i = 2$ and E_2 is cyclic. If $v_i = 2$ and E_2 is generalized quaternion, then Lemma 2.4(iv) implies that $|\langle [F(E)_2, R_i]\rangle| = |F(E)_2|/2$ and $|C_{F(E)_2}(R_i)| = 2$. Therefore, $|F(E)_2| = |\langle [F(E)_2, R_i]\rangle| \, |C_{F(E)_2}(R_i)|$. If F_1 denotes the Hall $2'$ subgroup of $F(E)$, then $F_1 = [R_i, F_1] \times C_{F_1}(R_i)$. Since $F(E)$ is nilpotent, it follows that $|F(E)| = |C_i| \, |\langle [(F(E), R_i]\rangle|$. Thus, for $i = 1,\ldots, t_u$ we obtain $|F| = 1 + 2\,|E| = 1 + 2u\,|C_i| \, |\langle [R_i, F(E)]\rangle|$.

For $i = 1,\ldots, t_u$, Lemma 2.4(iii) implies that there are integers a_i, b_i, with $b_i \geqslant 2$, such that $|C_i| \,\big|\, p^{a_i} - 1$ and $|P| = p^{a_i b_i}$. If v is an odd prime dividing b_i, then $|P|^{1/v}$ is an integer and $|P| - 1/(|P|^{1/v} - 1)$ is odd. It follows from Lemma 2.4(iii) and $|P| = 1 + 2\,|E|$ that $2|C_i|u/(u, v)$ divides $|P|^{1/v} - 1$. The previous paragraph now implies that $|\langle R_i, F(E)]\rangle| \geqslant (|P| - 1)/(u, v)(|P|^{1/v} - 1) > |P|^{2/3}/3$ if v is an odd prime dividing b_i. If $2 | b_i$, then Lemma 2.4(iii) implies that $(|C_i|u/(u, 2))| \;\; |P|^{1/2} - 1$. The previous paragraph implies that $4\,|\langle R_i, F(E)]\rangle| \geqslant |P|^{1/2} + 1$. If ud is divisible by 2 and v where v is an odd prime, then $|P|^{2/3}/3 > |P|^{1/2}/4$ Part (iii) now follows from (2.5.1).

(iv) If $\chi_m \in \mathscr{C}$ with $x_m = u$, then part (i) of this lemma implies that $\chi_m = \zeta^E$ where ζ is a faithful linear character of $F(E)/\ker \zeta$. Let $g = |F(E)/\ker \zeta|$. Since $F(E)$ is cyclic, $\ker \zeta$ is the unique subgroup of index g in $F(E)$. Hence, if $\chi_{m'} \in \mathscr{C}$ with $x_{m'} = u$, $\chi_{m'} = (\zeta')^E$, where ζ' is a faithful linear character of $F(E)/\ker \zeta'$, and $|F(E)/\ker \zeta'| = |F(E)/\ker \zeta|$, then ζ' and ζ are algebraic conjugates. Therefore, χ_m and $\chi_{m'}$ are algebraic conjugates. Let $g = v_1^{r_1} \cdots v_s^{r_s}$ denote the factorization of g into distinct prime powers where $r_i \geqslant 1$ for $i = 1 \dots s$. Let ϕ denote the Euler function. Since ζ^E is irreducible of degree u, $\phi(g) = ru$. It follows that $\chi_m = \zeta^E$ has r distinct algebraic conjugates so that $r = s_m$.

If $|E|$ is odd and $x_m = u$, then $\phi(g)$ is even and ug is odd. In particular, s_m is even. If $\chi_m \in \mathscr{C}$, then $s_m = 2$ implies that $2u = \phi(g) = \prod_{i=1}^{s} v_i^{r_i - 1}(v_i - 1)$. $\operatorname{Det} \chi_m = 1_E, x_m = u$, and part (iii) imply that $(g, u) = 1$. Now gu odd implies that $s = 1$ and $g = v_1 = 1 + 2u$. Part (iv) follows from the previous paragraph.

3

Throughout this section we assume that G is a group of minimal order such that G satisfies the hypothesis but not the conclusion of Theorem 1. Therefore, G satisfies Hypothesis 1′ with $C_G(P) = P$. We use the notation of Section 1. It follows from Section 1 that $N = EP$ is a Frobenius group where $|E| = n$, $|P| = q = 2n + 1$ and G is simple. Therefore, $N = EP$ satisfies Hypothesis 2. It follows from the results in Section 2 that N satisfies Lemma 2.3 or 2.4. G will be said to satisfy *Hypothesis* 3 if $N = EP$ satisfies Lemma 2.4. In particular, if n is odd, then G satisfies Hypothesis 3.

If n is even and E_2 is cyclic, let $E_2 = \langle y \rangle$. If β is a faithful irreducible character of E_2, then $\beta(y) = \alpha$ where α is a primitive $|E_2|$th root of unity, and β^i, $i = 1, \dots, |E_2|$, is the full set of irreducible characters of E_2. Proposition 1 implies that Λ_N is induced from a non-principal character of $C_G(P) = P$. It follows that $\Lambda_{E_2} = |E/E_2| \sum_{i=1}^{|E_2|} \beta^i$, whence $\det \Lambda(y) = \alpha^{(|E_2|/2)(|E_2|+1)|E/E_2|} = -1$. This contradicts Proposition 1. Therefore, E_2 is generalized quaternion if n is even.

The following description of the irreducible characters of N and G is based on Leonard [7]. We also use the fact that Λ_N is irreducible and $2n = q - 1$. N has exactly two irreducible characters λ and λ' which are induced from non-principal characters of P. Let $\mathscr{C}$ denote the set of the remaining irreducible characters of N. If $\chi_m \in \mathscr{C}$, then $P \subseteq \ker \chi_m$. Since Λ_N is irreducible, we may assume $\Lambda_N = \lambda$. There is another exceptional character Λ' such that $\Lambda'_N = \lambda'$. Let D denote the set of all non-exceptional irreducible characters of G which do not vanish on $P^\#$. If $X_m \in D$, then $X_m(y) = d_m$ for all $y \in P^\#$ and d_m is a non-zero integer. All other irreducible characters of G vanish on $P^\#$.

If $\chi_j \in \mathscr{C}$, let $x_j = \chi_j(1)$. Following Leonard's work [7], for $X_m \in D$ we define integers e_m, f_{mj}, and f_m by $(X_m, \lambda^G) = e_m$, $(X_m, \chi_j^G) = f_{mj}$, and $f_m = \sum_{\mathscr{C}} f_{mj} x_j$. The argument in [7] implies that $(X_m, (\lambda')^G) = e_m$. Since G

is simple, $e_m \geqslant 1$ if $X_m \neq 1_G$. Since $\Lambda_N = \lambda$ and $\Lambda'_N = \lambda'$, the argument in [7] also implies the following equalities:

$$f_m = e_m + d_m, \tag{3.1}$$

$$\sum_D d_m f_{mj} = x_j, \tag{3.2}$$

$$\sum_{\mathscr{C}} x_j^2 = n, \tag{3.3}$$

$$\sum_D d_m f_m = n; \tag{3.4}$$

$$\sum_D d_m^2 = n. \tag{3.5}$$

LEMMA 3.1. *Let* $A = \{X_m | X_m \in D, d_m > 0,$ *and* $X_m \neq 1_G\}$ *and let* $B = \{X_m | X_m \in D, d_m < 0\}$.

(i) If $X_m \in B$, then $f_{mj} = 0$, for all j and $X_m(1) = -2d_m n$. Moreover, $\sum_A f_m d_m = n - 1$.

(ii) Let $R = \sum_B (\Lambda\bar{\Lambda}, X_m) X_m$, then there are non-negative integers w, w', r, r' such that

$$\Lambda\bar{\Lambda} = 1_G + \sum_A d_m X_m + w\Lambda + w'\Lambda' + R,$$

$$\Lambda\bar{\Lambda}' = -\sum_B d_m X_m + r\Lambda + r'\Lambda' + R.$$

Moreover, $w + w' = r + r' - 1$.

(iii) $\sum_A (e_m - d_m) d_m + w + w' + \sum_B (\Lambda\bar{\Lambda}, X_m) 2|d_m| = 0$.

Proof. Let $\chi_j \in \mathscr{C}$. Both λ and λ' vanish off P and $P \subseteq \ker \chi_j$. It follows that $(\lambda\bar{\lambda}', \chi_j) = 0$ and $(\lambda\bar{\lambda}, \chi_j) = x_j$. Therefore, $(\Lambda\bar{\Lambda}'_N, \chi_j) = (\lambda\bar{\lambda}', \chi_j) = 0$ and $(\Lambda\bar{\Lambda}_N, \chi_j) = x_j$. Hence, if T is an irreducible character of G such that $(\Lambda\bar{\Lambda}', T) \neq 0$, then $(T, \chi_j^G) = 0$.

(i) Statement (2.1) [7] implies that $-d_m X_m \subseteq \Lambda\bar{\Lambda}'$ if $d_m < 0$. It follows that $f_{mj} = 0$ if $d_m < 0$. Equality (3.1) now implies that $X_m(1) = -2d_m n$ if $X_m \in B$. Equality (3.4) implies $\sum_A d_m f_m = n - 1$.

(ii) Let $X_m \in A$, then $e_m \geqslant 1$ and (3.1) imply that $f_{mj} > 0$ for some j.

Therefore, $(\Lambda\bar{\Lambda}', X_m) = 0$. Now the equation preceding (2.1) [7] implies $(\Lambda\bar{\Lambda}, X_m) = d_m$. Let T be an irreducible character which vanishes on $P^\#$. $T_N = (T, \lambda^G)(\lambda + \lambda') + \sum_{\mathscr{C}}(T, \chi_j^G)\chi_j$ implies that $(T, \lambda^G) = \sum_{\mathscr{C}}(T, \chi_j^G)x_j$. Therefore, $(\Lambda\bar{\Lambda}', T) = 0$. Since $\Lambda\bar{\Lambda} - \Lambda\bar{\Lambda}'$ vanishes off conjugates of $P^\#$ and T vanishes on conjugates of $P^\#$, $(\Lambda\bar{\Lambda}, T) = (\Lambda\bar{\Lambda}', T) = 0$. Statement (2.2) [7] implies $w + w' = r + r' - 1$. Statement (2.1) [7] implies that $(\Lambda\bar{\Lambda}', X_m) = (\Lambda\bar{\Lambda}, X_m) - d_m$ for $X_m \in B$. Part (ii) now follows.

(iii) Since $\Lambda(1) = n$, (i) and (ii) imply that $n^2 = 1 + \sum_A d_m(2e_m n + f_m) + (w + w')n + \sum_B 2|d_m|(\Lambda\bar{\Lambda}, X_m)n$. $\sum_A d_m f_m = n - 1$, whence $n - 1 = \sum_A 2d_m e_m + (w + w') + \sum_B 2(\Lambda\bar{\Lambda}, X_m)|d_m|$. Now $2e_m = f_m + e_m - d_m$ implies that $\sum_A 2d_m e_m = \sum_A d_m(e_m - d_m) + \sum_A f_m d_m = \sum_A d_m(e_m - d_m) + n - 1$. Part (iii) follows.

Let $A_1 = \{X_m | X_m \in A \text{ and } d_m > e_m\}$. A large portion of this section is devoted to showing that A_1 is empty. If A_1 is empty, a short argument similar to that used in [3] may be used to prove Theorem 1.

Assume A_1 is not empty. Lemma 3.1(i) implies that $d_m > 0$ if $f_{mj} \neq 0$. Therefore, (3.2) implies that $x_j \geqslant f_{mj} d_m$. Let $X_m \in A_1$, then (3.1) implies $2d_m > f_m = \sum_{\mathscr{C}} f_{mj} x_j \geqslant \sum_{\mathscr{C}} f_{mj}^2 d_m$. It follows that there is exactly one $\chi_j \in \mathscr{C}$ such that $f_{mj} \neq 0$. Moreover, $f_{mj} = 1$ and $d_m > x_j/2$. Hence, (3.2) implies that if $X_{m'} \in A_1 - \{X_m\}$, then $f_{m'j} = 0$ if $f_{mj} = 1$. For $X_m \in A_1$, let χ_m denote the $\chi_j \in \mathscr{C}$ such that $f_{mj} \neq 0$. Let $\mathscr{C}_1$ be the set of such χ_m. There is a 1–1 correspondence between $X_m \in A_1$ and $\chi_m \in \mathscr{C}_1$, and $X_{m|_N} = e_m(\lambda + \lambda') + \chi_m$. Therefore, $X_{m|_E} = 2e_m\rho_E + \chi_{m|_E}$ where ρ_E denotes the regular character of E. It is direct to show that $\det 2\rho_E = 1_E$. Proposition 1 implies that $\det X_m = 1_G$. It follows that $\det \chi_{m|_E} = 1_E$. We have shown

If X_m and χ_m are corresponding characters in A_1 and $\mathscr{C}_1$, then $d_m + e_m = x_m = f_m$, $d_m > x_m/2$, and $\det \chi_{m|_E} = 1_E$. (3.6)

If $\chi_m \in \mathscr{C}_1$, then $e_m \geqslant 1$ implies that $x_m \geqslant 3$. If $\mathscr{C}_1$ is non-empty, let k be defined by $\sum_{A_1} f_m^2 = \sum_{\mathscr{C}_1} x_m^2 = (n-2)/k$. Let $\gamma = \max\{d_m/e_m | X_m \in A_1\}$. If A_1 is empty, then let $\gamma = 1$. Equation (3.1) implies

$$d_m \leqslant \frac{\gamma f_m}{\gamma + 1} \quad \text{and} \quad \frac{d_m - e_m}{e_m} \leqslant \gamma - 1 \quad \text{if} \quad X_m \in A_1. \tag{3.7}$$

If G satisfies Hypothesis 3, let $|E/F(E)| = u$. Lemma 2.4 implies that $|P| = p^{ud}$ and every odd prime dividing u divides $|Z_1|$ where Z_1 denotes the Hall $2'$ subgroup of $Z(E)$. E_2 is generalized quaternion if n is even. Thus, Lemma 2.4(iv) implies that $u = 2u_1$ where u_1 is odd if n is even. If n is odd, then ud is odd. Assume that A_1 is non-empty and G satisfies Hypothesis 3. Let $\chi_m \in \mathscr{C}_1$, then Lemma 2.5 and (3.6) imply that $x_m | u$, $x_m \geqslant 3$, and χ_m is a character of N/Z_1P. It follows that $u/(u, |E_2|) \geqslant 3$ and $|Z_1| \geqslant 3$ if A_1 is non-empty. We have shown

$$\sum_{A_1} f_m^2 \leqslant \sum_{\mathscr{C}_1} x_m^2 \leqslant \frac{n-2}{|Z_1|} \leqslant \frac{n-2}{3} \qquad \text{if } G \text{ satisfies Hypothesis 3.} \quad (3.8)$$

LEMMA 3.2. *Let Γ be defined by $\Gamma = \{x | x \in G - \bigcup_G (P^{\#})^g\}$. The following conditions are satisfied.*

(i) *If $x \in \Gamma$, then $|\Lambda(x)| \leqslant 1 + \sum_A d_m f_m X_m(x)/X_m(1)$.*

(ii) $\sum_\Gamma |\Lambda(x)|^3 < \sum_\Gamma \Lambda^2(x) + (1 + \sum_{A_1} (d_m f_m (d_m - e_m)/e_m n))(|G| n/2q)$
$< \sum_\Gamma \Lambda^2(x) + (1 + \gamma(\gamma - 1)/(\gamma + 1)k)(|G|n/2q)$

(iii) *Let $\Gamma' = \{x | x \in \Gamma,\ |\Lambda(x)| \neq 0, 1\}$. If $\gamma = 1$, then n is odd and $\Gamma' = \{1\}$. If $\gamma \neq 1$, then $\sum_{\Gamma'} \Lambda^2(x) \leqslant (\gamma - 1)\gamma^2 n |G|/2k(\gamma + 1)^2 q$.*

Proof. An argument similar to that used in [3] implies that $\Lambda(x) = \Lambda'(x)$ and $\Lambda(x)$ is an integer if $x \in \Gamma$. Therefore, $\sum_\Gamma \Lambda(x)\bar{\Lambda}(x) = \sum_\Gamma \Lambda^2(x) = \sum_\Gamma \Lambda\Lambda'(x)$.

(i) Let $x \in \Gamma$ and $y \in P^{\#}$, then $1 + \sum_{A \cup B} X_m(x) X_m(y) + \Lambda(x)\Lambda(y) + \Lambda'(x)\Lambda'(y) = 0$. It follows that

$$\Lambda(x) - \sum_B d_m X_m(x) = 1 + \sum_A d_m X_m(x) \text{ if } x \in \Gamma. \qquad (3.2.1)$$

If $x_1, x_2, x_3 \in G$, then let c_{x_1, x_2, x_3} denote the number of ordered pairs $(x_1^{g_1}, x_2^{g_2})$ such that $x_1^{g_1} x_2^{g_2} = x_3$. Let y and $y' \in P^{\#}$ where y' is not conjugate to y^{-1}. If $x \varepsilon \Gamma$, then Eq. (2.15) [2] implies that

$$c_{y, y^{-1}, x^{-1}} = \frac{|G|}{q^2} \alpha_x \qquad \text{and} \qquad c_{y, y', x^{-1}} = \frac{|G|}{q^2} \beta_x,$$

where

$$\alpha_x = 1 + \sum_{A \cup B} \frac{d_m^2 X_m(x)}{X_m(1)} + \frac{(q-n)\Lambda(x)}{n}$$

and

$$\beta_x = 1 + \sum_{A \cup B} \frac{d_m^2 X_m(x)}{X_m(1)} - \frac{n\Lambda(x)}{n}.$$

Lemma 3.1 implies that if $X_m \in B$, then $X_m(1) = -2d_m n$. Therefore, (3.2.1) yields

$$1 + \sum_{A \cup B} \frac{d_m^2 X_m(x)}{X_m(1)} = 1 - \sum_B \frac{d_m X_m(x)}{2n} + \sum_A \frac{d_m^2 X_m(x)}{X_m(1)}$$
$$= \frac{q - \Lambda(x)}{2n} + \sum_A d_m X_m(x) \left(\frac{1}{2n} + \frac{d_m}{X_m(1)} \right).$$

Equation (3.1) implies that $1/2n + d_m/X_m(1) = f_m q/2nX_m(1)$ if $X_m \in A$. It follows that $1 + \sum_{A \cup B} (d_m^2 X_m(x)/X_m(1)) = (1/2n)(q - \Lambda(x) + \sum_A q d_m f_m X_m(x)/X_m(1))$. We see that $\beta_x = (q/2n)(1 - \Lambda(x) + \sum_A d_m f_m X_m(x)/X_m(1))$ and $\alpha_x = (q/2n)(1 + \Lambda(x) + \sum_A (d_m f_m X_m(x)/X_m(1)))$. Now $\beta_x \geqslant 0$, $\alpha_x \geqslant 0$, and $\Lambda(x)$ an integer imply (i).

(ii) Lemma 3.1(ii) implies that $(\Lambda\bar{\Lambda}, X_m) = d_m$ if $X_m \in A$. Hence, $\sum_{P\#} \Lambda\bar{\Lambda}(x)\, \bar{X}_m(x) = d_m(qn - n^2)$ implies that $\sum_\Gamma \Lambda^2(x)\, X_m(x) = |G|\, d_m n/q$. Part (i) now yields

$$\sum_\Gamma |\Lambda(x)|^3 \leqslant \sum_\Gamma \Lambda^2(x) + \frac{n|G|}{q} \sum_A \frac{d_m^2 f_m}{X_m(1)}. \tag{3.2.2}$$

If $X_m \in A$, then equality (3.1) implies that

$$\frac{d_m^2 f_m}{X_m(1)} < \frac{d_m f_m (d_m - e_m) + d_m f_m e_m}{2e_m n}.$$

Lemma 3.1(i) and $d_m \leqslant e_m$ for $X_m \in A - A_1$ now imply that

$$\sum_A \frac{d_m^2 f_m}{X_m(1)} < \sum_A \frac{d_m f_m}{2n} + \sum_A \frac{d_m f_m (d_m - e_m)}{2e_m n}$$
$$\leqslant \frac{n-1}{2n} + \sum_{A_1} \frac{d_m f_m (d_m - e_m)}{2e_m n}.$$

Therefore, (3.2.2) now yields

$$\sum_\Gamma |\Lambda(x)|^3 < \sum_\Gamma \Lambda^2(x) + \left(1 + \sum_{A_1} \frac{d_m f_m (d_m - e_m)}{e_m n} \right) \frac{|G|\, n}{2q}.$$

If $X_m \in A_1$, then (3.7) implies that $d_m f_m (d_m - e_m)/e_m n \leqslant (\gamma - 1)\, \gamma f_m^2/(\gamma + 1)\, n$. It follows that

$$\sum_{A_1} \frac{d_m f_m (d_m - e_m)}{e_m n} \leqslant \frac{(\gamma - 1)\, \gamma}{(\gamma + 1)\, n} \sum_{A_1} f_m^2 < \frac{(\gamma - 1)\, \gamma}{(\gamma + 1)\, k}.$$

Therefore, (ii) is proved.

(iii) If $X_m \in A$, then (3.1) implies that $X_m(1) = 2e_m n + f_m = f_m(n+1) + (e_m - d_m)\, n$. It follows that

$$\frac{f_m}{X_m(1)} = \frac{1}{n+1} + \frac{(d_m - e_m)\, n}{X_m(1)(n+1)}.$$

Moreover, if $x \in \Gamma$, then

$$\frac{f_m d_m X_m(x)}{X_m(1)} = \frac{d_m X_m(x)}{n+1} + \frac{d_m X_m(x)(d_m - e_m)\, n}{X_m(1)(n+1)}.$$

Therefore, if $x \in \Gamma$, then Lemma 3.1(ii) implies that

$$\begin{aligned} 1 + \sum_A \frac{d_m f_m X_m(x)}{X_m(1)} &= 1 + \sum_A \frac{d_m X_m(x)}{n+1} + \sum_A \frac{d_m(d_m - e_m)\, n X_m(x)}{(n+1)\, X_m(1)} \\ &= \frac{1}{n+1} \left(\Lambda^2(x) - (w + w')\, \Lambda(x) + n - R(x) \right. \\ &\qquad \left. + \sum_A \frac{d_m(d_m - e_m)\, n X_m(x)}{X_m(1)} \right). \end{aligned}$$

It now follows from part (i) of this lemma that

$$|\Lambda(x)|\,(n+1) \leqslant n + \Lambda^2(x) - (w+w')\Lambda(x) - R(x) + \sum_A \frac{d_m(d_m - e_m)\, n X_m(x)}{X_m(1)}.$$

Since $(n - |\Lambda(x)|)(|\Lambda(x)| - 1) = (n+1)|\Lambda(x)| - n - \Lambda^2(x)$, we may use the previous inequality to obtain

$$\begin{aligned} &(n - |\Lambda(x)|)(|\Lambda(x)| - 1) + (w + w')\, \Lambda(x) + R(x) + \sum_{A - A_1} \frac{(e_m - d_m)\, d_m X_m(x)\, n}{X_m(1)} \\ &\qquad \leqslant \sum_{A_1} \frac{(d_m - e_m)\, d_m n X_m(x)}{X_m(1)}. \end{aligned}$$

Now $\Lambda^2(x) = \Lambda\bar{\Lambda}(x) \geqslant 0$ for $x \in \Gamma$ implies that

$$\begin{aligned} &\sum_\Gamma (n - |\Lambda(x)|)(|\Lambda(x)| - 1)\, \Lambda\bar{\Lambda}(x) + \sum_\Gamma (w + w')\, \Lambda^3(x) \\ &\qquad + \sum_\Gamma R(x)\, \Lambda\bar{\Lambda}(x) + n \sum_{A - A_1} \sum_\Gamma \frac{(e_m - d_m)\, d_m X_m(x)\, \Lambda\bar{\Lambda}(x)}{X_m(1)} \\ &\qquad \leqslant n \sum_{A_1} \sum_\Gamma \frac{(d_m - e_m)\, d_m X_m(x)\, \Lambda\bar{\Lambda}(x)}{X_m(1)}. \end{aligned}$$

It was shown in part (ii) that $\sum_\Gamma X_m(x)\, A\bar{A}(x) = d_m|G|n/q$ if $X_m \in A$. If $X_m \in A - A_1$, then $e_m - d_m \geqslant 0$, and (3.1) imply that $f_m \leqslant 2e_m$. In particular, $X_m(1) \leqslant e_m(q+1)$ if $X_m \in A - A_1$. It follows that

$$n \sum_{A-A_1} \sum_{\Gamma} \frac{X_m(x)\, A\bar{A}(x)\, d_m(e_m - d_m)}{X_m(1)} \geqslant \frac{n^2\,|G|}{q(q+1)} \left(\sum_{A-A_1} \frac{d_m^2(e_m - d_m)}{e_m} \right) \geqslant 0. \tag{3.2.4}$$

If $X_m \in A_1$, then (3.7) implies that

$$\frac{nd_m^2(d_m - e_m)}{X_m(1)} < \frac{n(\gamma - 1)\, d_m^2}{2n} \leqslant \frac{(\gamma-1)\,\gamma^2 f_m^2}{2(\gamma+1)^2}.$$

Since $\gamma = 1$ if A_1 is empty, we obtain

$$\begin{aligned} \sum_{A_1} \sum_{\Gamma} \frac{nX_m(x)\, A\bar{A}(x)\, d_m(d_m - e_m)}{X_m(1)} &\leqslant \frac{(\gamma-1)\,\gamma^2 n\,|G|}{2(\gamma+1)^2 q} \sum_{A_1} f_m^2 \\ &= \frac{(\gamma-1)\,\gamma^2\,|G|(n-2)\,n}{2(\gamma+1)^2 kq}. \end{aligned} \tag{3.2.5}$$

If $X_m \in B$, then $\sum_{P^\#} A\bar{A}\bar{X}_m(y) = (qn - n^2)\, d_m$ implies that $\sum_\Gamma A\bar{A}\bar{X}_m(x) = (A\bar{A}, X_m)\,|G| + |d_m|(n+1)\,|G|/q$. It follows that

$$\sum_{\Gamma} A\bar{A}R(x) \geqslant (R, R)\,|G| \geqslant 0. \tag{3.2.6}$$

If n is odd and $y \in P^\#$, then $A\bar{A}(y) = \lambda\bar{\lambda}(y) = (n+1)/2$. Hence, $w = w'$ and we obtain

$$\sum_{\Gamma} A^3(x)(w + w') = 2w^2\,|G| + \frac{(n+1)\, w\,|G|}{q} \geqslant 0 \qquad \text{if } n \text{ is odd.} \tag{3.2.7}$$

If n is even, then $A\bar{A}'(y) = \lambda\lambda'(y) = -n/2$ for $y \in P^\#$. It follows that $r = r'$ in Lemma 3.1(ii). Since Lemma 3.1 implies that $w + w' = 2r - 1$, we see that $r \geqslant 1$. It follows that

$$\sum_{\Gamma} 2rA^3(x) = \sum_{\Gamma} A\bar{A}'(x)(r\bar{A} + r\bar{A}')(x) = 2r^2\,|G| - \frac{r|G|n}{q}.$$

Now $r \geqslant 1$ implies that

$$\sum_{\Gamma} A^3(x) \geqslant r|G| - \frac{n|G|}{2q} \geqslant \frac{(3n+2)\,|G|}{2q} > \frac{|G|3}{4}.$$

Since $w+w'=2r-1\geqslant 1$, we obtain

$$\sum_{\Gamma}(w+w')A^3(x)>\frac{3|G|}{4}\qquad\text{if } n \text{ is even.}\tag{3.2.8}$$

Inequalities (3.2.3)–(3.2.8) now yield

$$|G|\left((R,R)+2w^2+\frac{n^2}{q(q+1)}\sum_{A-A_1}\frac{d_m^2(e_m-d_m)}{e_m}\right)$$
$$+\sum_{\Gamma}(|A(x)|-1)(n-|A(x)|)A\bar{A}(x)\leqslant\frac{\gamma^2(\gamma-1)|G|n(n-2)}{(\gamma+1)^2\,2kq}$$
$$\text{if } n \text{ is odd,}$$
$$\frac{3|G|}{4}+\sum_{\Gamma}(|A(x)|-1)(n-|A(x)|)A\bar{A}(x)\leqslant\frac{\gamma^2(\gamma-1)|G|n(n-2)}{(\gamma+1)^2\,2kq}$$
$$\text{if } n \text{ is even.}\tag{3.2.9}$$

Assume $\gamma=1$. Since $(|A(x)|-1)(n-|A(x)|)A\bar{A}(x)\geqslant 0$ for $x\in\Gamma$, (3.2.9) implies that n is odd. Moreover, $e_m\geqslant d_m$ for $X_m\in A-A_1$ now implies that $(|A(x)|-1)(n-|A(x)|)A\bar{A}(x)=0$ for all $x\in G$. Proposition 1 now implies that $\Gamma'=\{1\}$.

For the rest of this proof we assume $\gamma\neq 1$. The conditions on G imply that $|G|=nq(rq+1)$ where $r\geqslant 1$. Thus, $A(1)=n$ implies that $|G|/4>(n-2)A^2(1)$. If $x\in\Gamma'-\{1\}$, then $(|A(x)|-1)(n-|A(x)|)\geqslant n-2$ since G is simple. It follows that $|G|/4+\sum_{\Gamma}(|A(x)|-1)(n-|A(x)|)A\bar{A}(x)>(n-2)\sum_{\Gamma'}A^2(x)$. Hence, (3.2.9) implies that $\sum_{\Gamma'}A^2(x)<|G|(\gamma-1)\gamma^2n/2(\gamma+1)^2kq$ unless n is odd and $(R,R)+2w^2=0$.

We may assume n is odd and $(R,R)+2w^2=0$. If

$$(n-2)A^2(1)\leqslant\frac{|G|n^2}{q(q+1)}\left(\sum_{A-A_1}\frac{d_m^2(e_m-d_m)}{e_m}\right),$$

then (3.2.9) and an argument similar to that used in the preceding paragraph will again imply that $\sum_{\Gamma'}A^2(x)\leqslant|G|(\gamma-1)\gamma^2n/2(\gamma+1)^2kq$. Therefore, we assume that

$$(n-2)n^2=(n-2)A^2(1)>\frac{|G|n^2}{q(q+1)}\sum_{A-A_1}\frac{d_m^2(e_m-d_m)}{e_m}.$$

Since $w=w'$ if n is odd, Lemma 3.1(iii) and $(R,R)=w=0$ now imply that $\sum_{A-A_1}(e_m-d_m)d_m=\sum_{A_1}d_m(d_m-e_m)\geqslant 2$. Therefore, there is a

$X_{m_0} \in A - A_1$ such that $e_{m_0} > d_{m_0}$. It follows that $(e_{m_0} - d_{m_0})\, d_{m_0}/e_{m_0} \geqslant \frac{1}{2}$. Therefore, (3.2.9) and $e_m \geqslant d_m$ for $X_m \in A - A_1$ imply that

$$\frac{|G|\, n^2}{q(q+1)} \sum_{A-A_1} \frac{d_m^2(e_m - d_m)}{e_m} \geqslant \frac{|G|\, d_{m_0} n^2}{2q(q+1)}.$$

Thus, $(n-2)\,A^2(1) > |G|\, d_{m_0} n^2/2q(q+1)$ implies that $|G| = nq(q+1)$, and $d_{m_0} = 1$. Now $e_{m_0} \geqslant 2$, and equality (3.1) imply that $X_{m_0}(1) = 2ne_{m_0} + e_{m_0} + 1 = e_{m_0} q + 1$. Since $X_{m_0}^2(1) < |G|$, $e_{m_0} < n$. However, $X_{m_0}(1)$ divides $nq(q+1)$. Clearly, $(q+1, e_{m_0} q + 1)$ divides $e_{m_0} - 1$, $(2ne_{m_0} + e_{m_0} + 1, n)$ divides $e_{m_0} + 1$, and $(X_{m_0}(1), q) = 1$. It follows that $(e_{m_0} - 1)(e_{m_0} + 1) \geqslant e_{m_0} q + 1$. This contradicts $e_{m_0} < n$.

COROLLARY 3.3. *G satisfies Hypothesis 3. If n is even, then* $|E/F(E)| = 2u_1$ *is odd,* $u_1 \geqslant 3$, *and* $\gamma > 4$.

Proof. G satisfies Hypothesis 3 if n is odd. Therefore, we will assume n is even.

Recall that $A(x)$ is an integer if $x \in \Gamma$. Let $\Gamma_+ = \{x | x \in \Gamma$ and $A(x) \geqslant 1\}$ and $\Gamma_- = \{x | x \in \Gamma$ and $A(x) \leqslant -1\}$. $(A, 1_G) = 0$, $(A, A) = 1$, and $A_N = \lambda$ imply that $-\sum_{\Gamma_-} |A(x)| + \sum_{\Gamma_+} |A(x)| = |G|/q$ and $\sum_{\Gamma_-} |A(x)|^2 + \sum_{\Gamma_+} A^2(x) = |G|\, n/q$. Subtracting the first equality from the second yields

$$\sum_{\Gamma_-} (|A(x)|^2 + |A(x)|) + \sum_{\Gamma_+} (A^2(x) - |A(x)|) = \frac{|G|(n-1)}{q}. \qquad (3.3.1)$$

Clearly $\sum_{\Gamma_+} (A^2(x) - |A(x)|) \leqslant \sum_{\Gamma'} A^2(x)$ where Γ' is defined in Lemma 3.2(iii). Therefore, Lemma 3.2(iii) implies that

$$\sum_{\Gamma_+} (A^2(x) - |A(x)|) \leqslant \frac{|G|\, \gamma^2(\gamma - 1)\, n}{(\gamma+1)^2\, 2kq} < \frac{|G|\, \gamma(\gamma-1)\, n}{(\gamma+1)\, 2kq}.$$

Now $\sum_{\Gamma_-} (|A(x)|^2 + |A(x)|) \leqslant 2 \sum_{\Gamma_-} |A(x)|^3$ and (3.3.1) imply

$$2 \sum_{\Gamma_-} |A(x)|^3 > \frac{|G|(n-1)}{q} - \frac{|G|\, \gamma(\gamma-1)\, n}{(\gamma+1)\, 2kq}. \qquad (3.3.2)$$

It was shown in the proof of Lemma 3.2(iii) that $\sum_\Gamma A^3(x) \geqslant ((3n+2)/2q)\,|G|$ if n is even. It follows that $\sum_{\Gamma_+} |A^3(x)| \geqslant ((3n+2)/2q)\,|G| + \sum_{\Gamma_-} |A(x)|^3$ whence $\sum_\Gamma |A^3(x)| \geqslant ((3n+2)/2q)\,|G| + 2\sum_{\Gamma_-} |A(x)|^3$. Lemma 3.2(ii), $\sum_\Gamma A^2(x) = |G|\, n/q$, and (3.3.2) now imply that

$$\frac{(3n+2)\,|G|}{2q} + \frac{|G|(n-1)}{q} - \frac{|G|(\gamma-1)\,\gamma n}{2k(\gamma+1)\,q} < \frac{|G|\, 3n}{2q} + \frac{|G|\, \gamma(\gamma-1)\, n}{2k(\gamma+1)\, q}.$$

We obtain

$$\frac{\gamma(\gamma-1)}{(\gamma+1)\,k} > 1. \tag{3.3.3}$$

If $N/P = EP/P$ contains a normal cyclic subgroup of index 2, then Theorems 9.11 and 9.12 [2] imply that every character in $\mathscr{C}$ has degree 1 or 2. However, (3.6) implies that A_1 is empty in this case and this contradicts (3.3.3). Hence, if G does not satisfy Hypothesis 3, then $N = EP$ satisfies Lemma 2.3(i), (ii), or (iii).

If Lemma 2.3(i) is satisfied, then direct computation implies that $\{1, 1, 1, 3, 2, 2, 2\}$ is the set of degrees of characters in $\mathscr{C}$. It follows that $A_1 = \{X_1\}$ where $f_1 = 3$, $d_1 = 2$ and $\gamma = 2$. Moreover, $f_1^2 = 9$ implies that $k = 22/9$. Substitution in (3.3.3) provides a contradiction.

Assume Lemma 2.3(ii) or (iii) is satisfied. Let Z_1 denote the Hall $2'$ subgroup of $Z(E)$, then $(n/|Z_1|, |Z_1|) = (24, 11)$ or $(48, 23)$. If $\chi_m \in \mathscr{C}$, then $x_m \mid |E/Z(E)|$. Hence, $(x_m, |Z_1|) = 1$. If $\chi_m \in \mathscr{C}_1$, then (3.6) implies that det $\chi_{m|_E} = 1_E$. If $w \in Z_1$, then $\chi_m(w) = x_m \alpha$ where α is a $|Z_1|$th root of unity. Thus, $(x_m, |Z_1|) = 1$ implies that $\alpha = 1$ and χ_m is an irreducible character of N/Z_1P. It follows that $k \geqslant |Z_1|$. Inequality (3.3.3) now implies that $\gamma > |Z_1| + 1$. If $\chi_m \in A_1$ where $d_m/e_m = \gamma$ and χ_m is the corresponding character in $\mathscr{C}_1$, then χ_m is an irreducible character of N/Z_1P. Therefore, (3.6) implies that $\gamma + 1 \leqslant f_m$ and $f_m^2 = x_m^2 \leqslant n/|Z_1|$. Now $|Z_1|^2 < \gamma^2 < f_m^2 \leqslant n/|Z_1|$ clearly contradicts $(n/|Z_1|, |Z_1|) = (24, 11)$ or $(48, 23)$.

Therefore, G satisfies Hypothesis 3. Since n is even, $|E/F(E)| = 2u_1$ where u_1 is odd. Inequalities (3.8) and (3.3.3) imply that $\gamma(\gamma-1)/(\gamma+1)\,3 > 1$ so that $\gamma > 4$.

If X_m and χ_m are corresponding characters in A_1 and $\mathscr{C}_1$, let r_m and s_m denote the number of distinct algebraic conjugates of X_m and χ_m. It follows from the discussion preceding (3.6) that $s_m = r_m$. Since G satisfies Hypothesis 3, we see that r_m is even if n is odd.

LEMMA 3.4. *Assume that A_1 is non-empty and $X_j \in A_1$. Let T_j be the sum of the distinct algebraic conjugates of X_j, then*

$$\sum_{\Gamma} |A(x)|\, T_j^2(x) < |G| \left(r_j - \frac{2d_j^2 r_j^2}{q} + r_j^2 e_j^2 \left(1 + \sum_{A_1} \frac{f_m^2(d_m - e_m)}{e_m n}\right) + \frac{f_j^2 \gamma r_j^2}{2n} \right).$$

Proof. Since T_j is a sum of distinct algebraic conjugates, T_j is integer valued. $(T_j, T_j) = r_j$ and $\sum_{P\#} T_j^2(y) = 2n(d_j r_j)^2$ imply that $\sum_{\Gamma} T_j^2(x) =$

$|G|\,r_j-(d_jr_j)^2\,2\,|G|/q$. If $X_m \in A$, then $T_j^2(y)\,X\overline{X_m(y)} > 0$ for $y \in P^{\#}$ whence $\sum_{\Gamma} T_j^2\,\overline{X}_m(x) < |G|(T_j^2, X_m)$. Therefore, Lemma 3.2(i) implies that

$$\sum_{\Gamma} |A(x)|\,T_j^2(x) < |G|\left\{r_j - \frac{2d_j^2\,r_j^2}{q} + \sum_{A} \frac{d_m f_m(T_j^2, X_m)}{X_m(1)}\right\}. \tag{3.4.1}$$

Let $A_{1,j}$ denote the set of algebraic conjugates of X_j. Let $\mathscr{C}_{1,j}$ denote the corresponding characters in $\mathscr{C}_1$. Now $X_{j|_N} = e_j(\lambda+\lambda')+\chi_j$ implies that $T_{j|_N} = r_je_j(\lambda+\lambda')+S$ where $S=\sum_{\mathscr{C}_{1,j}}\chi_{j'}$. It follows that $T_{j|_N}^2 = T_j\overline{T}_{j|_N} = e_j^2\,r_j^2(\lambda\bar{\lambda}+\lambda'\bar{\lambda}'+\lambda\bar{\lambda}'+\lambda'\bar{\lambda})+2e_jr_j(\lambda+\lambda')\,S+S\overline{S}$. If $\chi_s \in \mathscr{C}$, then $P \subseteq \ker\chi_s$ whence $(\lambda'\bar{\lambda}, \chi_s) = (\lambda\bar{\lambda}', \chi_s) = ((\lambda+\lambda')\,S, \chi_s) = 0$. Moreover, $(\lambda\bar{\lambda}, \chi_s) = (\lambda'\bar{\lambda}', \chi_s) = x_s$. It follows that $(T_{j|_N}^2, \chi_s) = 2e_j^2\,r_j^2x_s + (S\overline{S}, \chi_s)$. We now obtain,

$$\sum_{A} (T_j^2, X_m)\,f_{ms}x_s \leqslant 2e_j^2\,r_j^2x_s^2 + (S\overline{S}, \chi_s)\,x_s. \tag{3.4.2}$$

Let $\mathscr{C}^{\#} = \mathscr{C} - \{1_N\}$. Lemma 3.1 and Eq. (3.2) imply that $(X_m, 1_N^G) = 0$ if $X_m \in A$. Therefore, $\sum_A(T_j^2, X_m)\,f_m = \sum_A(T_j^2, X_m)(\sum_{\mathscr{C}^{\#}} f_{ms}x_s) = \sum_{\mathscr{C}^{\#}}(\sum_A(T_j^2, X_m)\,f_{ms}x_s)$. Now (3.4.2) and $S\overline{S} = \sum_{\mathscr{C}^{\#}}(S\overline{S}, \chi_s)\,\chi_s + r_j1_N$ imply

$$\sum_{A} (T_j^2, X_m)\,f_m \leqslant 2e_j^2\,r_j^2(n-1) + r_j^2f_j^2 - r_j. \tag{3.4.3}$$

If $X_m \in A$, then (3.1) implies that $d_m/X_m(1) < 1/2n + (d_m-e_m)/2e_mn$. Hence, $d_m - e_m \leqslant 0$ for $X_m \in A - A_1$ and (3.4.3) imply

$$\begin{aligned}\sum_{A} \frac{(T_j^2, X_m)\,f_m d_m}{X_m(1)} &< \frac{1}{2n}\,(2e_j^2r_j^2(n-1) + r_j^2f_j^2 - r_j)\\ &\quad + \sum_{A_1} \frac{f_m(d_m-e_m)(T_j^2, X_m)}{2e_mn}.\end{aligned} \tag{3.4.4}$$

If $X_m \in A_1$, then let χ_m denote the corresponding character in $\mathscr{C}_1$. Since $f_m = x_m$, (3.4.2) implies that $f_m(T_j^2, X_m) \leqslant 2f_m^2r_j^2\,e_j^2 + (S\overline{S}, \chi_m)\,x_m$. It follows that

$$\begin{aligned}\sum_{A_1} \frac{f_m(d_m-e_m)(T_j^2, X_m)}{2e_mn} &\leqslant e_j^2r_j^2 \sum_{A_1} \frac{(d_m-e_m)\,f_m^2}{e_mn}\\ &\quad + \sum_{A_1} \frac{(d_m-e_m)(S\overline{S}, \chi_m)\,x_m}{2e_mn}.\end{aligned}$$

Inequality (3.7) implies that

$$\sum_{A_1} \frac{(d_m-e_m)(S\overline{S}, \chi_m)\,x_m}{2e_mn} \leqslant \frac{(\gamma-1)}{2n} \sum_{\mathscr{C}_1} (S\overline{S}, \chi_m)\,x_m < \frac{(\gamma-1)(r_jf_j)^2}{2n}.$$

Inequalities (3.4.1), and (3.4.4) now imply that

$$\sum_{\Gamma} |\Delta(x)| T_j^2(x) < |G| \left\{ r_j - \frac{2d_j^2 r_j^2}{q} + e_j^2 r_j^2 \left(1 + \sum_{A_1} \frac{(d_m - e_m) f_m^2}{e_m n} \right) + \frac{\gamma (r_j f_j)^2}{2n} \right\}.$$

LEMMA 3.5. *If* A_1 *is non-empty and* $X_j \in A_1$, *let* β_j *be defined by* $\sum_\Gamma \overline{X_j(x)}\, |\Delta(x)| = \beta_j |G|\, n/q$. *The following conditions are satisfied.*

$$\text{(i)} \quad \beta_j < \min \left\{ \left(\frac{2}{r_j}\right)^{1/2}, \left(\frac{1}{r_j}\left(\frac{\gamma^2(\gamma-1)}{(\gamma+1)^2 k} + 1\right)\right)^{1/2} \right\},$$

$$\text{(ii)} \quad \left(1 + \sum_{A_1} \frac{d_m f_m (d_m - e_m)}{e_m n}\right)\left(\frac{1}{r_j} + \frac{\gamma f_j^2}{2n} + e_j^2 \left(1 + \sum_{A_1} \frac{f_m^2 (d_m - e_m)}{e_m n}\right)\right) > \min\{(d_j - \beta_j)^2, d_j^2\}.$$

Proof. (i) We may assume $\beta_j > 0$. Let T_j be the sum of distinct algebraic conjugates of X_j. Then $\sum_\Gamma T_j(x) |\Delta(x)| = r_j \beta_j |G|\, n/q$ since $\Delta(x)$ is an integer for $x \in \Gamma$. As in the proof of Lemma 3.4, we obtain

$$\sum_{\Gamma} T_j^2(x) = |G| \left(r_j - \frac{2r_j^2 d_j^2}{q} \right) < \frac{|G|\, 2r_j n}{q}. \tag{3.5.1}$$

It was shown in the proof of Lemma 3.2 that $\sum_\Gamma \Delta^2(x) = |G|\, n/q$. The Cauchy–Schwartz inequality and $\sum_\Gamma |\Delta(x)|\, T_j(x) = \beta_j r_j |G|\, n/q$ now imply that $|G|^2\, 2r_j n^2/q^2 > \beta_j^2 r_j^2\, |G|^2 n^2/q^2$. It follows that $\beta_j < (2/r_j)^{1/2}$.

Let $\Gamma_1 = \{x \mid x \in \Gamma, |\Delta(x)| = 1$, and $T_j(x) > 0\}$, $\Gamma_2 = \{x \mid x \in \Gamma,\ |\Delta(x)| > 1$, and $T_j(x) > 0\}$ and $\Gamma_3 = \Gamma - (\Gamma_1 \cup \Gamma_2)$. Let h, v, and w be defined by $\sum_{\Gamma_1} |\Delta(x)|\, T_j(x) = h |G|\, n/q$, $\sum_{\Gamma_2} |\Delta(x)|\, T_j(x) = v |G|\, n/q$ and $\sum_{\Gamma_2} T_j^2(x) = w^2 |G|\, n/q$. Clearly $r_j \beta_j |G|\, n/q = \sum_\Gamma |\Delta(x)|\, T_j(x) \leqslant (h + v) |G|\, n/q$. Since $\Gamma_2 \subseteq \Gamma'$, Lemma 3.2(iii) and the Cauchy–Schwartz inequality imply that $\alpha w^2 |G|^2 n^2/q^2 \geqslant v^2 |G|^2 n^2/q^2$ where $\alpha = (\gamma - 1)\, \gamma^2/(\gamma + 1)^2\, 2k$. Hence, $v \leqslant \alpha^{1/2} w$ so we obtain

$$r_j \beta_j \leqslant (w\alpha^{1/2} + h) \tag{3.5.2}$$

Inequality (3.5.1) implies that $w^2 |G|\, n/q < |G|\, 2r_j n/q$. Therefore, (3.5.2) implies that $\beta_j < ((\gamma - 1)\, \gamma^2/(\gamma + 1)^2\, r_j k)^{1/2}$ if $h \leqslant 0$. Hence, we may assume $h > 0$.

$(T_j, 1_G) = 0$ implies that $\sum_\Gamma T_j(x) = -2r_j d_j |G|/q$. Thus, $T_j(x) > 0$ for

$x \in \Gamma_2$ and $\sum_{\Gamma_1} T_j(x) = \sum_{\Gamma_1} T_j(x)|A(x)| = h|G|n/q$ imply that $\sum_{\Gamma_3} |T_j(x)| \geqslant (hn + 2r_j d_j)|G|/q$. It follows that $\sum_{\Gamma_1 \cup \Gamma_3} |T_j(x)| \geqslant (2hn + 2r_j d_j)|G|/q$. Since $P^{\#}$ is a TI-set, $|\Gamma| = |G|((q-2)/q)$. The Cauchy–Schwartz inequality now implies that

$$\sum_{\Gamma_1 \cup \Gamma_3} T_j^2(x) \geqslant \frac{(2hn + 2r_j d_j)^2 |G|}{q(q-2)} > \frac{2h^2 n |G|}{q}.$$

It follows from (3.5.1) that $w^2 < 2(r_j - h^2)$. Therefore (3.5.2) implies that $r_j \beta_j < h + (2\alpha(r - h^2))^{1/2}$. Since $0 \leqslant h \leqslant r_j^{1/2}$, elementary calculus may be applied to the function $f(x) = x + (2\alpha(r - x^2))^{1/2}$ to show that $r_j \beta_j < ((2\alpha + 1) r_j)^{1/2}$. It follows that

$$\beta_j < \left(\frac{1}{r_j}(2\alpha + 1)\right)^{1/2} = \left(\frac{1}{r_j}\left(\frac{\gamma^2(\gamma - 1)}{(\gamma + 1)^2 k} + 1\right)\right)^{1/2}.$$

(ii) It was shown in the proof of Lemma 3.2 that $\sum_\Gamma A^2(x) X_j(x) = |G| d_j n/q$. Hence, $\sum_\Gamma A^2(x) T_j(x) = |G| r_j d_j n/q$. Now $\sum_\Gamma |A(x)| T_j(x) = |G| r_j \beta_j n/q$ implies

$$\sum_\Gamma |A(x)|(|A(x)| - 1) T_j(x) = \frac{|G| r_j(d_j - \beta_j) n}{q} \tag{3.5.3}$$

We may write

$$\sum_\Gamma |A(x)|(|A(x)| - 1) T_j(x) = \sum_\Gamma \{|A(x)|^{1/2}(|A(x)| - 1)\}\{|A(x)|^{1/2} T_j(x)\}.$$

$X_j \in A_1$ implies that $d_j \geqslant 2$, therefore, part (i) implies that $d_j - \beta_j > 0$. The Cauchy–Schwartz inequality and (3.5.3) now imply

$$\left(\sum_\Gamma |A(x)|(|A(x)| - 1)^2\right)\left(\sum_\Gamma |A(x)| T_j^2(x)\right) \geqslant \frac{|G|^2 r_j^2 (d_j - \beta_j)^2 n^2}{q^2}. \tag{3.5.4}$$

Lemma 3.2(ii) and $A(x)$ an integer for $x \in \Gamma$ imply that

$$\sum_\Gamma |A(x)|(|A(x)| - 1)^2 \leqslant \sum_\Gamma |A(x)|^3 - \sum_\Gamma |A(x)|^2 < \frac{n|G|}{2q} \times \left(1 + \sum_{A_1} \frac{d_m f_m (d_m - e_m)}{e_m n}\right).$$

Lemma 3.4 and (3.5.4) now imply that

$$\frac{r_j^2\, n\,|G|^2}{2q}\left(1+\sum_{A_1}\frac{d_m f_m(d_m-e_m)}{e_m n}\right)$$
$$\times\left(\frac{1}{r_j}-\frac{2d_j^2}{q}+e_j^2\left(1+\sum_{A_1}\frac{(d_m-e_m)f_m^2}{e_m n}\right)+\frac{f_j^2\gamma}{2n}\right)$$
$$\geqslant |G|^2\,\frac{r_j^2(d_j-\beta_j)^2 n^2}{q^2}.$$

It follows that

$$\left(1+\sum_{A_1}\frac{d_m f_m(d_m-e_m)}{e_m n}\right)\left(\frac{1}{r_j}+e_j^2\left(1+\sum_{A_1}\frac{(d_m-e_m)\,f_m^2}{e_m n}\right)+\frac{f_j^2\gamma}{2n}\right)$$
$$\geqslant\frac{(d_j-\beta_j)^2\,2n+2d_j^2}{q}>\min\{(d_j-\beta_j)^2,d_j^2\}.$$

Since EP satisfies Hypothesis 2, Lemma 2.4 implies that $|P|=p^{ud}$ where $|E/F(E)|=u$. Further $p\neq 3$.

Assume that n is even; it follows from Corollary 3.3 that $u=2u_1$ where u_1 is odd and $u_1\geqslant 3$. Further E_2 is a generalized quaternion. Hence, $|P|\neq 5^6$ so that $|P|\geqslant 7^6$ if n is even. Straightforward computations with logarithms imply that $2n+1=p^{ud}>50u^4$. It follows that $u^4/2n\leqslant 1/50$ if n is even.

If n is odd, then $|P|=p^{ud}$ where ud is odd and $p\equiv 3 \pmod 4$. It follows that $|P|\geqslant 7^{ud}$. We will show that either $u^7\leqslant 2n$ or $|P|=7^3$ if n is odd. Since $u^7>2n$ implies that $u^7\geqslant 2n+1=|P|\geqslant 7^{ud}$, we see $u^7/2n\leqslant 1$ if $ud\geqslant 7$. $((|P|,u)=1$ so that $p\geqslant 11$ if $u=7$.) Since ud is odd, we may assume $ud=u=3$ or 5 and $|P|\neq 7^3$. Lemma 2.4 implies that u divides $|Z(E)|$ if $u=3$ or 5. Therefore, $|P|=p^u\equiv 1 \pmod{u^2}$ and $p\equiv 3 \pmod 4$. If $du=3$, then $p=7$ or $p\geqslant 19$. If $ud=5$, then $p\geqslant 11$. It follows that either $2n\geqslant u^7$ or $|P|=7^3$.

We have shown

$$\begin{aligned}&\frac{u^4}{2n}\leqslant\frac{1}{50} &&\text{if } n \text{ is even,}\\ &\frac{1}{|P|}<\frac{1}{2n}\leqslant\frac{1}{u^7} &&\text{if } n \text{ is odd and } |P|\neq 7^3.\end{aligned}\tag{3.9}$$

If n is odd, let $A_1'=\{X_m\mid X_m\in A_1$, and $f_m<u$ or $f_m=u$ and $r_m=2\}$. If A_1' is non-empty, let $\mathscr{C}_1'$ denote the subset of $\mathscr{C}_1$ corresponding to characters in A_1'. If X_m and χ_m are corresponding characters in A_1' and C_1', then $r_m=s_m$. Let t_u

denote the number of distinct primes dividing u. Lemma 2.5 and (3.6) now imply that

$$\begin{aligned}\sum_{A'_1} f_m^2 = \sum_{\mathscr{P}'_1} x_m^2 &\leqslant 0 && \text{if } |P| = 7^3\\ &\leqslant 2u^2 && \text{if } u \text{ is a prime}\\ &\leqslant \frac{3t_u n}{|P|^{2/3}} + 2u^2 && \text{if } u \text{ is not a prime.} \qquad (3.10)\end{aligned}$$

PROPOSITION 3.6. *A_1 is empty and n is odd.*

Proof. Corollary 3.3 implies that it is sufficient to show that A_1 is empty. We will assume that A_1 is non-empty.

Since G satisfies Hypothesis 3, (3.7) and (3.8) imply that

$$\sum_{A_1} \frac{(d_m - e_m)\, d_m f_m}{e_m n} \leqslant \frac{\gamma(\gamma-1)}{(\gamma+1)\,k} \leqslant \frac{\gamma(\gamma-1)}{3(\gamma+1)}$$

and

$$\sum_{A_1} \frac{(d_m - e_m)\, f_m^2}{e_m n} \leqslant \frac{(\gamma-1)}{3}.$$

Let $X_j \in A_1$, then Lemma 3.5 and the previous inequalities imply that

$$\begin{aligned}&\left(1 + \frac{(\gamma-1)\,\gamma}{3(\gamma+1)}\right)\left(1 + \frac{\gamma f_j^2}{2n} + e_j^2\left(1 + \frac{\gamma-1}{3}\right)\right)\\ &\quad\geqslant \left(1 + \frac{(\gamma-1)\,\gamma}{(\gamma+1)\,k}\right)\left(\frac{1}{r_j} + \frac{\gamma f_j^2}{2n} + e_j^2\left(1 + \frac{\gamma-1}{k}\right)\right)\\ &\quad> \min\{(d_j - \beta_j)^2, d_j^2\}. \qquad (3.6.1)\end{aligned}$$

Lemma 2.5 and (3.6) imply that if $X_j \in A_1$, then $d_j + e_j = f_j = x_j$ and $x_j | u$.

We first show that $u \neq 3$. If $u = 3$ and $X_j \in A_1$, then $d_j = 2$, $e_j = 1$, and $\gamma = 2$. Since $u = 3$, n is odd so either $r_j = 2$ or $r_j \geqslant 4$. If $|P| = 7^3$, then $\gamma f_j^2/2n = 18/2n = 1/19$. If $|P| \neq 7^3$, then (3.9) implies that $\gamma f_j^2/2n \leqslant 18/2n < 0.01$. If $r_j \geqslant 4$ for some $X_j \in A_1$, then Lemma 3.5 implies that

$$\beta_j < \left(\frac{1}{4}\left(\frac{\gamma^2(\gamma-1)}{(\gamma+1)\,k} + 1\right)\right)^{1/2} \leqslant \left(\frac{1}{4}\left(\frac{4}{27} + 1\right)\right)^{1/2} < 0.54.$$

Substitution in (3.6.1) now implies that $2 > (1+\frac{2}{9})(\frac{1}{4}+\frac{1}{19}+\frac{4}{3}) > (2-0.54)^2$. This is a contradiction. However, $r_j = 2$ for all $X_j \in A_1$ implies that $A_1 = A_1'$ where A_1' is defined before inequality (3.10). Whence (3.10) yields that $|P| \neq 7^3$ and $(n-2)/k = \sum_{A_1} f_m^2 = 2u^2 = 18$. It follows from (3.9) that $k > 60$. Lemma 3.5 implies that

$$\beta_j \leqslant \left(\frac{1}{2}\left(\frac{\gamma^2(\gamma-1)}{(\gamma+1)^2 k}+1\right)\right)^{1/2} \leqslant \left(\frac{1}{2}\left(\frac{4}{9\cdot 60}+1\right)\right)^{1/2} < 0.71.$$

Since $\gamma f_j^2/2n < 0.01$, substitution in (3.6.1) yields $(1+2/(3\cdot 60))(\frac{1}{2}+0.01+(1+\frac{1}{60})) > (2-0.71)^2$. Again, this is a contradiction.

Thus, we may assume $u \geqslant 5$. Since $\gamma f_j^2 < u^3/2n$, (3.9) implies that $\gamma f_j^2/2n < 0.004$. Let $X_1 \in A_1$ where $d_1/e_1 = \gamma$. We will show that $d_1 \leqslant e_1 + 2$. This condition is clearly satisfied if $d_1 < 4$. Lemma 3.5 implies that $\beta_1 < (2)^{1/2}$. Since $(\gamma-1)\gamma/(\gamma+1)3 < (\gamma-1)/3$, (3.6.1) implies that $((2+\gamma)/3)(1.004) + e_1^2((2+\gamma)/3)^2 > (d_1 - 2^{1/2})^2 \geqslant (d_1-2)^2 + 1.1d_1 - 2$. If $((2+\gamma)/3)(1.004) > 1.1d_1 - 2$, then $\gamma \leqslant d_1$ easily yields $d_1 < 4$. Therefore, we may assume that $e_1((2+\gamma)/3) > d_1 - 2$. However, $\gamma = d_1/e_1$ whence $d_1 - 2 < e_1((2+\gamma)/3) = (2e_1+d_1)/3$. We obtain $2(d_1-e_1) < 6$. Since d_1 and e_1 are integers, $d_1 \leqslant e_1 + 2$. In particular, $\gamma \leqslant (e_1+2)/e_1 \leqslant 3$. Corollary 3.3 now implies that n is odd.

Since n is odd, x_1 is odd. Thus, $d_1 + e_1 = x_1$ implies that $d_1 = e_1 + 1$ so that $\gamma \leqslant 2$.

Let A_1' be the subset of A_1 defined before (3.10). It follows from (3.9) that $|P|^{-2/3} < u^{-14/3}$. Since $u \geqslant 5$, $t_u \leqslant u/5$ where t_u is the number of distinct primes dividing u. Therefore, (3.9), (3.10), and $u \geqslant 5$ imply that

$$\sum_{A_1'} f_m^2 \leqslant 3un(5u^{14/3})^{-1} + 4nu^{-5} < 0.08nu^{-2}. \tag{3.6.2}$$

Since $\gamma \leqslant 2$, it follows from (3.7) and (3.6.2) that

$$\sum_{A_1'} \frac{(d_m-e_m)\, f_m d_m}{e_m n} \leqslant \frac{2}{3n}\sum_{A_1'} f_m^2 < 0.06u^{-2} \qquad \text{and}$$

$$\sum_{A_1'} \frac{(d_m-e_m)\, f_m^2}{e_m n} < 0.08u^{-2}.$$

If $A_1 - A_1'$ is empty, let $\gamma' = 1$. If $A_1 - A_1'$ is non-empty, then let $\gamma' = \max\{(d_m/e_m) \mid X_m \in A_1 - A_1'\}$. It is direct to show that $f_m d_m(d_m-e_m)/e_m \leqslant f_m^2(d_m-e_m)/e_m \leqslant (\gamma'-1) f_m^2$ for $X_m \in A_1 - A_1'$. Thus (3.8) implies that

$$\sum_{A_1-A_1'} \frac{f_m d_m(d_m-e_m)}{e_m n} \leqslant \sum_{A_1-A_1'} \frac{f_m^2(d_m-e_m)}{e_m n} \leqslant \frac{(\gamma'-1)}{n}\sum_{A_1} f_m^2 \leqslant \frac{\gamma'-1}{3}.$$

We may now use the results of the previous paragraph to obtain

$$\begin{aligned} \sum_{A_1} \frac{(d_m - e_m)\, d_m f_m}{e_m n} &\leqslant 0.06u^{-2} + \frac{\gamma' - 1}{3}, \\ \sum_{A_1} \frac{(d_m - e_m)\, f_m^2}{e_m n} &\leqslant 0.08u^{-2} + \frac{\gamma' - 1}{3}. \end{aligned} \tag{3.6.3}$$

If $X_j \in A_1$, then $\gamma \leqslant 2$, (3.6.3), and Lemma 3.5 imply

$$\left(1 + 0.06u^{-2} + \frac{\gamma' - 1}{3}\right)\left(r_j^{-1} + f_j^2 n^{-1} + e_j^2 \left(1 + 0.08u^{-2} + \frac{\gamma' - 1}{3}\right)\right)$$
$$> \min\{d_j^2, (d_j - \beta_j)^2\}. \tag{3.6.4}$$

We will now bound the left-hand side of (3.6.4). The left-hand side of (3.6.4) may be written

$$\left(\frac{2 + \gamma'}{3} + 0.06u^{-2}\right)(r_j^{-1} + f_j^2 n^{-1})$$
$$+ e_j^2 \left[\left(\frac{2 + \gamma'}{3}\right)^2 + 0.14u^{-2}\left(\frac{2 + \gamma'}{3}\right) + 0.0048u^{-4}\right].$$

By using $f_j \leqslant u$, $u \geqslant 5$, n odd, and (3.9), we obtain $0.06u^{-2} < 0.003$ and $f_j^2 n^{-1} < 0.001$. Now $r_j \geqslant 2$ since n is odd. Whence, $0.06u^{-2}(r_j^{-1} + f_j^2 n^{-1}) < 0.003(0.501)$. Further, $\gamma' \leqslant 2$ implies that $(2 + \gamma')/3(r_j^{-1} + f_j^2 n^{-1}) < (2 + \gamma')/3r_j + \frac{4}{3}(0.001)$. It follows that $((2 + \gamma')/3 + 0.06u^{-2})(r_j^{-1} + f_j^2 n^{-1}) < (2 + \gamma')/3r_j + 0.0029$. Now, $e_j^2(0.14u^{-2}((2 + \gamma')/3) + 0.0048u^{-4}) < (u^2/4)(0.14u^{-2}(\frac{4}{3}) + 0.0048u^{-4})) < 0.0468$ follows from $\gamma' \leqslant 2$, $e_j < f_j/2 \leqslant u/2$, $u \geqslant 5$, and (3.9). Hence, we see that

$$\left(1 + 0.06u^{-2} + \frac{\gamma' - 1}{3}\right)\left(r_j^{-1} + f_j^2 n^{-1} + e_j^2 \left(1 + 0.08u^{-2} + \frac{\gamma' - 1}{3}\right)\right)$$
$$< \frac{2 + \gamma'}{3r_j} + e_j^2 \left(\frac{2 + \gamma'}{3}\right)^2 + 0.0497.$$

Using this bound and (3.6.4), we obtain

$$0.0497 + \frac{\gamma' + 2}{3r_j} + e_j^2 \left(\frac{2 + \gamma'}{3}\right)^2 > \min\{d_j^2, (d_j - \beta_j)^2\} \quad \text{if } X_j \in A_1. \tag{3.6.5}$$

If $\gamma' = 1$, let $X_j = X_1$; then $d_1 = e_1 + 1$, $r_1 \geqslant 2$ and (3.6.2) imply that $k > 300$. Thus, Lemma 3.5(i) yields $\beta_1 < 0.71$ and $(d_1 - \beta_1)^2 > (e_1 + 0.29)^2$. Substitution in (3.6.5) now implies that $0.0497 + 0.5 + e_1^2 > (e_1 + 0.29)^2$. This contradicts $e_1 \geqslant 1$. Therefore, we may choose $X_2 \in A_1 - A_1'$ where $d_2/e_2 = \gamma'$.

Since $X_2 \in A_1 - A_1'$, $d_2 + e_2 = x_2 = u$ and $r_2 \geqslant 4$. It follows from Lemma 3.5 that $\beta_2 < 0.54$ since $\gamma^2(\gamma - 1)/(\gamma + 1)^2 k \leqslant 4/27$. Now $(2 + \gamma')/3 = (2e_2 + d_2)/3e_2$, $\gamma' \leqslant 2$, $r_2 \geqslant 4$, and (3.6.5) imply that $0.3831 + (2e_2 + d_2)^2/9 > (d_2 - 0.54)^2 \geqslant (d_2 - 1)^2 + 0.92d_2 - 0.71$. We obtain $d_2 = e_2 + 1$. However, substituting $2e_2 + d_2 = 3e_2 + 1$ and $d_2 = e_2 + 1$ in the previous inequality now yields $0.3831 + (3e_2 + 1)^2/9 > (e_2 + 0.46)^2$. It follows that $e_2 = 1$ whence $u = d_2 + e_2 = 2e_2 + 1 = 3$. This is a contradiction.

Proof of Theorem 1. Proposition 3.6 implies that A_1 is empty and n is odd. Lemma 3.2(iii) implies $|\Lambda(x)| = 1$ or 0 for $x \in \Gamma - \{1\}$. Since $e_m \geqslant d_m$ for $X_m \in A$, Lemma 3.1(iii) implies that $\Lambda\bar{\Lambda} = 1_G + \sum_A d_m X_m$ and $\sum_A (e_m - d_m)\, d_m = 0$. It follows that $e_m = d_m$ for $X_m \in A$. Now $f_m = e_m + d_m$ implies that $f_m = 2d_m$ for $X_m \in A$. It follows from Lemma 3.1(i) that $\sum_A d_m^2 = (n-1)/2$. The proof of Proposition 11 [3] may easily be adapted to show that $|G| = nq(q+1)$.

Since $|G| = nq(q+1)$ and n is odd, E_v is a Sylow v subgroup of G for every prime v dividing $|E|$. Let y_v be an element of order v in E_v. Assume $x \in C_G(y_v)$ where x has prime order r and $(r, v) = 1$. Theorem (17.4) [2] implies that $\Lambda(yx) = 0$. Since $\Lambda(x)$ is an integer, (6.4) [2] implies that $0 = \Lambda(xy) = \Lambda(x) \pmod{v}$. Lemma 3.2 (iii) implies that $\Lambda(x) \in \{0, \pm 1\}$. It follows that $\Lambda(x) = 0$. However, $\Lambda(1) \equiv \Lambda(x) \pmod{r}$ now implies that $r | n$. It easily follows that $|C_G(y)| \,\|\, n$ if $y \in E^{\#}$.

Let v be a prime dividing $|Z(E)|$, then $C_G(y_v) = E$. Since $E_v = G_v$ is cyclic, and G is simple, $N_G(\langle y_v \rangle) > E$. Therefore, $|N_G(\langle y_v \rangle)/E|$ is divisible by a prime s where $(s, n) = 1$. Let x be an element of order s in $N_G(\langle y_v \rangle)$, then x normalizes E. The previous paragraph implies that $|C_E(x)| = 1$. Theorem 10.2.1 [5] now implies that E is nilpotent. Since n is odd, E is cyclic. This is a contradiction.

References

1. R. Brauer, On groups whose order contains a prime number to the first power, I, II, *Amer. J. Math.* **64** (1942), 401–420, 421–440.
2. W. Feit, "Characters of Finite Groups," Benjamin, New York, 1967.
3. P. Ferguson, Linear groups of degree $(q-1)/2$, *J. Algebra* **63** (1980), 287 – 300.
4. P. Ferguson and S. Smith, Strongly self-centralizing Sylow 3-groups, *J. Algebra* **58** (1979), 572–580.
5. D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.

6. I. M. ISAACS, "Character Theory of Finite Groups," Academic Press, New York, 1976.
7. H. S. LEONARD, JR., Finite linear groups having an Abelian Sylow Subgroup, *J. Algebra* **20** (1972), 57–69.
8. H. S. LEONARD, JR., Finite linear groups having an Abelian Sylow Subgroup, II, *J. Algebra* **26** (1973), 368–382.
9. D. PASSMAN, "Permutation Groups," Benjamin, New York, 1968.
10. D. A. SIBLEY, Finite linear groups with a strongly self-centralizing Sylow subgroup, *J. Algebra* **36** (1975), 319–332.